August, 2023

AGE®

# Cyber Security Framework

Arranged by
**Autoboys and Apollo Studios**

Prepared for
**Automotive Glass Experts (AGE)**

www.automotiveglassexperts.com

# Table of Contents

# Overview

Automotive Glass Experts have designed the Automotive Glass Experts Cybersecurity Policy to comply with the NIST standards and have measures in place to meet CIS Control V7, meeting all of Implementation Group 1 requirements and aim to achieve and 80% compliance to Group 2 requirements within the next 2 financial years.

The following measures have been implemented in all five areas of cybersecurity preparedness as delineated by the NIST Cyber Security Framework, which are 1) Identify, 2) Protect, 3) Detect, 4) Respond, 5) Recover.

**Identify**

- We maintain necessary inventories, policies, and procedures to manage our asset/software portfolios. Cybersecurity dependencies are monitored to ensure key services delivery in critical functions, and resilience requirements are in place to mitigate risk to critical services.

- We identify internal risks and vulnerabilities, document internal and external cybersecurity threats and assess their potential impact to the supply chain. Our Risk committee continuously updates risk response priorities based on our risk register and our digital products undergo regular cybersecurity vulnerability reviews by an independent third party, specializing in threat and vulnerability assessments.

- The Cybersecurity Policy is approved by our C-Suite, and communicated to Management, IT staff, and all users accessing our systems.

- We have regular Cybersecurity Risk Management Review meetings to determine our organizational risk tolerance and improve on management's awareness towards sector-specific risks.

- We manage cybersecurity risk to our supply chain by coordinating responsibilities and communicating response & recovery plans with our external partners, including suppliers, contractors, and third-party partners.

**Protect**

- We use the industry's leading AI powered software, proving real-time vulnerability protection from malicious software, DDOS, and other cybersecurity attacks on all exposed ports, end-point devices and network nodes.

- We have detailed internal cybersecurity policies and processes to protect our products and services from cybersecurity threats. Our policies pertain to identities and credentials management, data security, and information management.

- We have regular training and education sessions with our staff and downstream partners, regarding cybersecurity, privacy, civil liberties, and obligations. Our privileged users, senior executives, and third-party stakeholders are informed of their roles and responsibilities, managed and controlled through acceptance of and adherence to our internal policies.

**Detect**

- We employ a combination of digital products to manage and monitor our environments which deliver a level of protection to our hardware and software assets, as well as information and data.

- We continuously assess whether appropriate detection capabilities are in place, and update policies, procedures and security that offer appropriate levels of protection and enable swift communication of vulnerabilities and risks within the organisation.

**Respond**

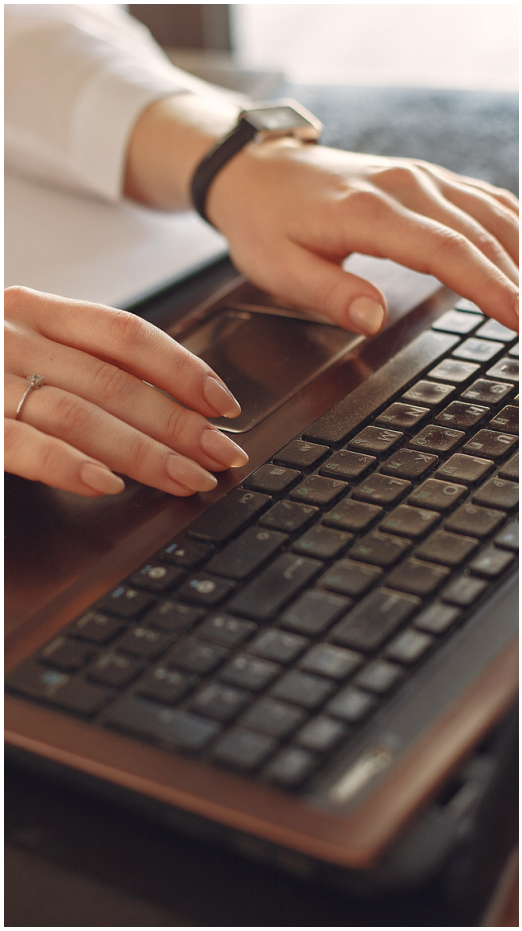
- We maintain and regularly update a Cybersecurity Incident Response Plan that delineates roles and responsibilities and coordinates actions in case of cybersecurity incidents. In the event of a cybersecurity incident, we determine investigation intensity based on available information from our detection systems. In the event of a major incident, the required forensics will be outsourced to an independent third party specialist.

**Recover**

We maintain and regularly update a Recovery Plan that delineates roles and responsibilities, restoration activities and communication requirements to manage public relations and company reputation.

**Overview**

Automotive Glass Experts is dedicated to creating a secure cyber environment to ensure appropriate protection for its assets and operations. The following requirements apply to all Automotive Glass Experts employees which act in unison to minimise vulnerabilities and risks coming from work environment, outsider access, or staff conduct.



# Workplace Cybersecurity Environment Policy

## Physical Security Policy

**Overview**

- Physical access controls define who is allowed physical access to Automotive Glass Experts facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems. Without physical access controls, there exists the possibility that information systems could be illegitimately, physically accessed and the security of the information they house could be compromised.

**Purpose**

This policy applies to all facilities of Automotive Glass Experts, within which information systems or information system components are housed. Specifically, it includes:

- Data centers or other facilities for which the primary purpose is the housing of IT infrastructure.
- Data rooms or other facilities, within shared purpose facilities, for which one of the primary purposes is the housing of IT infrastructure.
- Switch and wiring closets or other facilities, for which the primary purpose is not the housing of IT infrastructure.

**Policy Detail**

Access to facilities, information systems, and information system display mechanisms will be limited to authorized personnel only.

Authorization will be demonstrated with authorization credentials that have been issued by Automotive Glass Experts.

Access to facilities will be controlled at defined access points with locked doors and controlled access. Access to Automotive Glass Experts IT Department will be restricted to authorised individuals, managed by the main entry control point of the company.

Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorized personnel are required to authenticate themselves at these access points. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility, without prior authorization, and all deliveries and removals will be logged.

A list of authorized personnel will be established and maintained so that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall be reviewed and, where necessary, updated on at least an annual basis.

- If visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified, and must have their authorization verified before physical access is granted. Once access has been granted, visitors must be escorted, and their activities monitored at all times.

**Physical and Environmental Security**

- Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

- A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.

- Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

- All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.

- Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

# Workstation Configuration Policy

**Purpose**
The purpose of this policy is to enhance security and quality operating status for workstations utilized at Automotive Glass Experts. The workstations at Automotive Glass Experts provide a wide variety of services to process sensitive information for Automotive Glass Experts Insurance Customers. These devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure against such attacks. IT personnel are to utilize these guidelines when deploying all new workstation equipment.

Workstation users are expected to maintain these guidelines and to work collaboratively with IT resources to maintain the infrastructure in accordance with Policy framework.

The overriding goal of this policy is to reduce operating risk. Adherence to the Automotive Glass Experts Workstation Configuration Security Policy will:

- Eliminate configuration errors and reduce workstation outages.
- Reduce undocumented workstation configuration changes that tend to open up security vulnerabilities.
- Facilitate compliance and demonstrate that the controls are working.
- Protect Automotive Glass Experts data, networks, and databases from unauthorized use and/or malicious attack.

Therefore, all new workstation equipment that is owned and/or operated by Automotive Glass Experts must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all Automotive Glass Experts company-owned, company operated, or company-controlled workstation equipment. Additionally, new workstations, within Automotive Glass Experts facilities, will be managed at the sole discretion of IT. Non-sanctioned workstation installations, or use of unauthorized equipment that access networked resources on Automotive Glass Experts property, is strictly forbidden.

## Policy Detail

**Responsibilities**

Automotive Glass Experts Chief Technology Office has the overall responsibility for the confidentiality, integrity, and availability of Automotive Glass Experts data.

Other IT staff members, under the direction of the Director of IT, are responsible for following the procedures and policies within IT.

**Supported Technology**

All workstations will be centrally managed by Automotive Glass Experts IT Department and will utilize approved workstation configuration standards, which will be established and maintained by Automotive Glass Experts IT Department.

All established standards and guidelines for the Automotive Glass Experts IT environment are documented in an IT storage location.

The following outlines Automotive Glass Experts's minimum system requirements for workstation equipment.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the Director of IT.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. Automotive Glass Experts has deployed a patch management process; reference the Patch Management Policy (5-K).
- All workstations joined to the Automotive Glass Experts domain will automatically receive a policy update configuring the workstation to obtain future updates from our desktop management system.
- All systems within Automotive Glass Experts are required to utilize anti-virus, malware, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.
- All workstations will utilize the Automotive Glass Experts domain so that all general policies, controls, and monitoring features are enabled for each workstation. No system should be managed manually but should be managed through some central tool or model in order to efficiently manage and maintain system security policies and controls.
- Third-party applications need to be updated and maintained. So that software with security updates is not exposed to vulnerabilities for longer than necessary, a quarterly review will be performed.
- Third-party applications, including browsers, shall be updated and maintained in accordance with the Automotive Glass Experts patch management program.
- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the IT Department to guarantee the security of the workstations in accordance with the Automotive Glass Experts patch management program.

- Internet browsers on workstations will remain up to date. To ensure all browsers are up to date, the IT Department will perform quarterly reviews. If there is a reason the browser cannot be updated, due to conflicts with applications, these exceptions will be recorded.

- By default, all workstations joined to the Automotive Glass Experts domain will obtain local security settings through policies.

This policy is complementary to any previously implemented policies dealing specifically with security and network access to Automotive Glass Experts's network.

It is the responsibility of each employee of Automotive Glass Experts to protect Automotive Glass Experts's technology based resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to Automotive Glass Experts's public image.

Procedures will be followed to ensure resources are protected.

# Personal Device Policy

**Overview**
Acceptable use of personal devices at Automotive Glass Experts must be managed to ensure that access to Automotive Glass Experts's resources for business are performed in a safe and secure manner for participants of the Automotive Glass Experts personal devices program. A participant of the personal devices program includes, but is not limited to:

- Employees
- Contractors
- Board of Directors
- Volunteers
- Related constituents who participate in the personal devices program

This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

**Purpose**
This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data using their personal device. This policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the Automotive Glass Experts personal devices program which contains stored data owned by Automotive Glass Experts, and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any non-Automotive Glass Experts owned mobile device capable of storing corporate data and connecting to an unmanaged network

Refer to the Company and Personally Owned Mobile Device Procedure.

This policy addresses a range of threats to, or related to, the use of Automotive Glass Experts data, such as loss, theft, copyright violation, malware, non-compliance.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the Automotive Glass Experts network.

**Audience**
This policy applies to all Automotive Glass Experts employees, including full and part-time staff, Board of Directors, volunteers, contractors, freelancers, and other agents who utilize personally-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Automotive Glass Experts has built with its

members, suppliers, and other constituents. Consequently, employment at Automotive Glass Experts does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

**Policy Detail**
This policy applies to:

- Any privately owned wireless and/or portable electronic handheld equipment, hereby referred to as personal devices. Automotive Glass Experts grants potential participants of the personal devices program the privilege of purchasing and using a device of their choosing at work for their convenience.

- Related software that could be used to access corporate resources.

This policy is intended to protect the security and integrity of Automotive Glass Experts's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The Audience, as defined above, must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network. If users do not abide by this policy, Automotive Glass Experts reserves the right to revoke this privilege.

The following criteria will be considered initially, and on a continuing basis, to determine if the Audience is eligible to connect a personal smart device to the Automotive Glass Experts network.

- Management's permission and certification of the need and efficacy of personal devices for that Employee

- Sensitivity of data the Audience can access

- Legislation or regulations prohibiting or limiting the use of a personal smart device for Automotive Glass Experts business

- Audience's adherence to the terms of the Bring Your Own Device Agreement and this policy and other applicable policies

- Technical limitations

- Other eligibility criteria deemed relevant by Automotive Glass Experts or IT

**Responsibilities of Automotive Glass Experts**

- IT will centrally manage the personal devices program and devices including, but not limited to, onboarding approved users, monitoring personal devices connections, and terminating personal devices connections to company resources upon the users leave of employment or service to Automotive Glass Experts.

- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable.

- IT reserves the right to refuse, by non-physical means, the ability to connect mobile devices to Automotive Glass Experts and Automotive Glass Experts-connected

infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts Automotive Glass Experts's systems, data, users, and members at risk.

- IT will maintain enterprise IT security standards.

- IT retains the rights to inspect all mobile devices attempting to connect to the Automotive Glass Experts network through an unmanaged network (i.e. the Internet) using technology centrally managed by the IT Department.

- IT will install the Mobile VPN software required on Smart mobile devices, such as Smartphones, to access the Automotive Glass Experts network and data.

**Automotive Glass Experts's IT Department reserves the right to:**

- Install anti-virus software on any personal devices participating device

- Restrict applications

- Limit use of network resources

- Wipe data on lost/damaged devices or upon termination from the personal devices program or Automotive Glass Experts employment

- Properly perform job provisioning and configuration of personal devices participating equipment before connecting to the network

- Through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the Automotive Glass Experts network

**Responsibilities of personal devices Participants Security and Damages /R**

- All potential participants will be granted access to the Automotive Glass Experts network on the condition that they read, sign, respect, and adhere to the Automotive Glass Experts policies concerning the use of these devices and services (see Exhibit A).

- Prior to initial use on the Automotive Glass Experts network or related infrastructure, all personally owned mobile devices must be registered with IT.

- Participants of the personal devices program and related software for network and data access will, without exception:

a. Use secure data management procedures. All personal devices equipment, containing stored data owned by Automotive Glass Experts, must use an approved method of encryption during transmission to protect data.

b. Be expected to adhere to the same security protocols when connected with approved personal devices equipment to protect Automotive Glass Experts's infrastructure.

c. Automotive Glass Experts data is not to be accessed on any hardware that fails to meet Automotive Glass Experts's established enterprise IT security standards.

d. Ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied to personal devices use.

e. Utilize a device lock with authentication, such as a fingerprint or strong password, on each participating device. Refer to the Automotive Glass Experts password policy for additional information.

f. Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.

g. Passwords and confidential data should not be stored on unapproved or unauthorized non-Automotive Glass Experts devices.

h. Exercise reasonable physical security measures. It is the end users responsibility to keep their approved personal devices equipment safe and secure.

i. A device's firmware/operating system must be up-to-date in order to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of the owner.

j. Any non-corporate computers used to synchronize with personal devices equipment will have installed anti-virus and anti-malware software deemed necessary by Automotive Glass Experts's IT Department. Anti-virus signature files must be up to date on any additional client machines – such as a home PC – on which this media will be accessed.

k. IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.

l) If A) any personal devices device is lost or stolen, immediately contact Automotive Glass Experts IT; and, if B) any personal devices device is scheduled to be upgraded or exchanged, the user must contact IT in advance. IT will disable the personal devices and delete associated company data.

m) Personal devices equipment that is used to conduct Automotive Glass Experts business will be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's access.

n) Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Automotive Glass Experts's overarching security policy.

o)Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.

p. The user agrees to and accepts that his or her access and/or connection to Automotive Glass Experts's networks may be monitored to record dates, times, duration of access, etc. This is done to identify unusual usage patterns or other suspicious activity, and to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Automotive Glass Experts's highest priority.

q. Employees, Board of Directors, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of Automotive Glass Experts owned and installed hardware or software without the express approval of Automotive Glass Experts's IT Department.

r. The end user agrees to immediately report, to his/her manager and Automotive Glass Experts's IT Department, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of Automotive Glass Experts resources, databases, networks, etc.

**Third Party Vendors**
Third party vendors are expected to secure all devices with up-to-date anti-virus signature files and anti-malware software relevant or applicable to a device or platform. All new connection requests between third parties and Automotive Glass Experts require that the third party and Automotive Glass Experts representatives agree to and sign the Third Party Agreement. This agreement must be signed by the Vice President of the sponsoring department, as well as a representative from the third party who is legally empowered to sign on behalf of the third party. By signing this agreement, the third party agrees to abide by all referenced policies. The document is to be kept on file. All non-publicly accessible information is the sole property of Automotive Glass Experts.

**Help and Support**
Automotive Glass Experts's IT Department is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

# Electronic Communication Policy

**Purpose**
The purpose of this electronic communications policy is to:

- Inform users on the use of electronic resources
- Create rules for the use of electronic resources
- Provide for disciplinary action against Users who fail to comply with this policy; and
- Ensure and maintain the value and integrity of the company's equipment and network(s)

This policy creates rules that aim to limit or manage the risk associated with liability to Automotive Glass Experts coming from the staff's unlimited usage of electronic resources.

**Scope**
This policy applies to all Users as well as third parties that have temporary access to the company's e-mail, Internet access or network and who:

- Use the company's facilities to send and receive e-mail messages (including attachments thereto)
- Access the Internet and the Internet's services including but not limited to Jostle, the World Wide Web and Internet chat rooms; and
- Save, retrieve or print files, e-mail messages or other electronic documents to and/or from the company's network or a computer data storage media.

**Responsibility**
Users are personally responsible to abide by the rules created in this policy, and must delete all incoming e-mail messages that contain content or links to content that are not allowed in terms of this

The Automotive Glass Experts IT Support department is responsible for:

- The technical issues related to e-mail use and Internet access;
- Assisting the Company's management to conduct searches / monitoring of User's incoming and outgoing e-mail messages, stored messages, stored files and browsing habits;
- Causing all outgoing e-mail messages to contain the Company's official e-mail disclaimer;
- Scanning all incoming messages and file downloads for malicious codes such as viruses or Trojan Horses;
- Sustaining User's awareness of this and other Institutional policies related to the use of the Institution's electronic facilities

- The Human Resource Department is responsible for offering training for Users in the proper use of the Institution's electronic facilities (including activating the "out of office" e-mail feature).

- Automotive Glass Experts's management is responsible for taking any necessary action against User's who fail and/or refuse to abide by this policy

## Policy Details

**Right To Monitor**
With due regard to the South African Constitution and the Regulation of Interception of Communications Act, each and every User, when he or she accepts employment with Automotive Glass Experts, whether it be on contract or a permanent appointment, is deemed thereby to have given his or her consent that the Human Resources department of the Company may formally request CTS, without prior warning to:

- Intercept, monitor, block, delete, read and act upon any incoming or outgoing e-mail message addressed to or originating from the User;

- Intercept, monitor, read and act upon the User's Internet browsing habits, including the User's history files, web sites visited, files downloaded and stored by the User; and

- Intercept, monitor, block, delete, read and act upon any file, in whatever format, stored by a User on any computer or other facilities of the institution.

- The right to monitor is required by law since under certain conditions, the law enforcement of the country can instruct an institution to provide information, which will assist in its proper operation.

- The institution also has a right to monitor in the case where its interests have been threatened. Hence the Electronic Communications Policy specifically allows for scrutiny ONLY through the HR department of the company.

- In all other cases an individual's rights are upheld in that permission must be granted from the individual before information can be monitored.

- In general, transactional activities can be monitored as long as the content of the transaction is not compromised.

There are two ways in which monitoring may be performed:

In the first instance, the communication activity is monitored. Thus, as an example, the throughput of the computer network is monitored. The reason for doing so is to manage the capacity of the platform for the purposes of optimization. As a parallel, this is the same as managing traffic flow in a road system through the number of lanes and traffic light control. No actual data content or site connections are monitored.

In the second instance, the content of the transaction can be monitored together with the transaction source and destination. This type of monitoring can only be instituted by law enforcement, through a formal initiation by the HR department or with specific approval of the owner(s). The decision to monitor the communications of an individual shall firstly be approved by a committee consisting of the Direct of Human Resources, the Director/manager of Automotive Glass Experts, a legal representative of the company and a Union representative. A register shall be maintained by this committee recording all dates and activities with regard to the monitoring.

# Account Management Policy

**Purpose**
The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at Automotive Glass Experts.

**Audience**
This policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at Automotive Glass Experts, including all personnel affiliated with third parties with authorized access to any Automotive Glass Experts information system.

## Policy Detail

**Accounts**

- All accounts created must have an associated written request and signed management approval that is appropriate for the Automotive Glass Experts system or service.
- All accounts must be uniquely identifiable using the assigned username.
- Shared accounts on Automotive Glass Experts information systems are not permitted.
- Reference the Employee Access During Leave of Absence Policy for removing an employee's access while on a leave of absence or vacation.
- All default passwords for accounts must be constructed in accordance with the Automotive Glass Experts Password Policy.
- All accounts must have a password expiration that complies with the Automotive Glass Experts Password Policy.
- Concurrent connections may be limited for technical or security reasons.
- All accounts must be disabled immediately upon notification of any employee's termination.

**Account Management**
The following items apply to System Administrators or designated staff:

- Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.
- All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
- Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.

- All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.

- Information system accounts are to be reviewed monthly to identify inactive accounts. If an employee or third party account is found to be inactive for 30 days, the owners (of the account) and their manager will be notified of pending disablement. If the account continues to remain inactive for 15 days, it will be manually disabled.

- A list of accounts, for the systems they administer, must be provided when requested by authorized Automotive Glass Experts management.

- An independent audit review may be performed to ensure the accounts are properly managed.

# Acceptable Use Policy

**Purpose**
The purpose of this policy is to define appropriate usage of workstations and other network devices, Automotive Glass Experts network, and other equipment and to prevent intentional and unintentional misuse by Automotive Glass Experts employees.

**Acceptable use and general guidelines**
The following actions and content will be considered acceptable use of e-mail and Internet facilities by Users:

- Users shall use e-mail and Internet access primarily for business purposes related to the company.Private and personal use, in moderation, will be tolerated, subject to the rules detailed in this policy;
- Equipment, systems, services and software on the company's networks are to be used primarily for business purposes related to the company. Common sense and good judgement should guide personal and private usage;
- When forwarding or replying to e-mail messages, the contents of the original message should not be altered. If the contents need to be changed, then all changes must be clearly marked as such;
- The company has the right to limit the size of incoming and outgoing e-mail messages and attachments, downloads and other files and may block and delete e-mail messages, downloads, attachments or other files that are larger than the set maximum size. It is the responsibility of Users to limit the size of attachments and other files to prevent overloading of the electronic mail system resources;
- E-mail messages should be kept brief and formulated appropriately;
- Virus warnings or pop-ups that result from incoming e-mail or file downloads must be reported to the Support department immediately the following number: (010) 600 7901 /2;
- All outgoing e-mails must have the company's standard e-mail disclaimer at the end of the message.This e-mail disclaimer may not be removed or tampered with by Users;
- Users must check e-mail recipients prior to sending, forwarding or replying to messages. When distribution lists are used the sender should consider whether or not each group member really needs, or really should, receive the e-mail;
- The subject field of an e-mail message should relate directly to the contents or purpose of the message;
- Users must log-off or use screen savers with passwords in times of absence from a computer terminal to avoid improper and/or illegal use;

- If Users who are employees of the company are out of the office for more than one day, they should activate the "Out of Office" function. This informs the sender of an e-mail of a recipient's absence. The "Out of Office" message should include both the period of absence and an alternative contact person.

- Access to the Internet using Automotive Glass Experts equipment and facilities must pass through the Firewall. No party may connect to any other network while physically connected to the Automotive Glass Experts network.

**Policy Detail**
The following actions and content are not allowed and will lead to investigation and possibly disciplinary action:

- Sharing network logon usernames with or disclosing passwords to any third person(s);

- Fabricating a message or sender of a message;

- Intentionally bypassing the security mechanisms of the mail system or any other secure web site or network (e.g. creating bogus accounts);

- Modifying the internal mail transport mechanism to forge a routing path that a message takes through the Internet;
- Storing, downloading and propagating, printing, distributing, sending or accessing illegal content;

- Downloading, receiving or installing software applications not approved by the IT department;

- Knowingly burdening the company's network with non-work related data (e.g. forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server);

- Using automatic forwarding of e-mails ("Auto Rules") to any person without such person's consent;

- The creation, sending or forwarding of unsolicited mail (spam);

- Knowingly sending or forwarding messages and attachments that could be infected with malicious codes such as viruses, as well as spam; if in doubt please contact the IT department at the following number: (010) 600 7901/2;

- Using discs that may be infected with malicious code, without taking reasonable measures to ensure that the discs are safe to use;

- Accessing and using internet relay chat if such actions burden the Company's systems or prevent other Users from using them;

- Any non-business actions that knowingly prevent other Users from using e-mail or Internet access;

- Taking any of those steps or actions criminalised and detailed in Chapter XIII of the Electronic Communications and Transactions Act 25 of 2002, (sections 85, 86, 87, 88 and 89) including but not limited to hacking or developing, downloading and using any technology that may circumvent IT security measures;

- Any destructive and disruptive practices either via e-mail or the Internet;

- Indiscriminate storage and/or forwarding of e-mail, files, web sites and attachments for which permission has not been obtained from the originator or copyright holder;

- Any purposes that could reasonably be expected to cause directly or indirectly excessive strain on any computing facilities, or unwarranted or unsolicited interference with others;

- Sending, replying to or forwarding e-mail messages or other electronic communications which hides the identity of the sender or represents the sender as someone else;

- Users of the company's electronic mail systems who obtain access to materials of other organisations may not copy, modify or forward copyrighted materials, except under the specific copyright terms and conditions; and

- Using information, e-mail, files, downloads or data to commit fraud or any other criminal offence(s).

- Making illegal copies of the Company's software installation disks.

- Users may not set up any Internet Services (such as WWW, Telnet or FTP) within the Automotive Glass Experts network, nor assign any IP addresses to any devices without the express authority of IT Support.

**Consequences of Mis-use**

- Failure and/or refusal to abide by the rules detailed in this policy shall be deemed as misconduct and the Company may initiate the appropriate investigation and disciplinary action against Users. Such disciplinary action may vary from a verbal reprimand up to termination of employment depending on the seriousness of the offence.

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the organziation's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records).

- Observing authorized levels of access and utilizing only approved IT technology devices or services; and

- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities, after approval from organizational management, in consultation with organization IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;

- Unauthorized use or disclosure of organization information and resources;

- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;

- Attempting to represent the organization in matters unrelated to official authorized job duties or responsibilities;

- Connecting unapproved devices to the organization's network or any IT resource;

- Connecting organizational IT resources to unauthorized networks;

- Connecting to any wireless network while physically connected to the organization's wired network;

- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with organizational policies;

- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (organizations must recognize the inherent risk in using commercial email services as email is often used to distribute malware);

- Using an organization's IT resources to circulate unauthorized solicitations or advertisements for non-organizational purposes including religious, political, or not-for-profit entities;

- Providing unauthorized third parties, including family and friends, access to the organization's IT information, resources or facilities;

- Using orgnanization IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);

- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using organizational IT resources; and

- Tampering, disengaging, or otherwise circumventing an organization or third-party IT security controls.

- In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the organization's IT resources is not permissible.

- The organization may impose restrictions, at the discretion of their executive management, on the use of a particular IT resource. For example, the organization may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the organization's IT resources (e.g., personal USB drives, iPods).

- Users accessing the organization's applications and IT resources through personal devices must only do so with prior approval or authorization from the organization.

**Acceptable Use**
All uses of information and information technology resources must comply with organizational policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;

- Protecting organizational information and resources from unauthorized use or disclosure;

- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;

**Occasional and Incidental Personal Use**
Occasional, incidental and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the organization's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important.Organizations may revoke or limit this privilege at any time.

**Individual Accountability**
Individual accountability is required when accessing all IT resources and organization information.Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information, and must not be disclosed or shared.

**Restrictions on Off-Site Transmission and Storage of Information**
Users must not transmit restricted organization, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct the organization's business unless explicitly authorized. Users must not store restricted organizational, non-public, personal, private, sensitive, or confidential information on a non-organizational issued device, or with a third-party file storage service that has not been approved for such storage by the organization.

Devices that contain organizational information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

**User Responsibility for IT Equipment**
Users are routinely assigned or given access to IT equipment in connection with their official duties.This equipment belongs to the organization and must be immediately returned upon request or at the time an employee is separated from the organization.

Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the organization. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The organization has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

**Use of Social Media**
The use of public social media sites to promote organizational activities requires written pre-approval from the Public Information Office (PIO). Approval is at the discretion of the PIO and may be granted upon demonstration of a business need, and a review and approval of service agreement terms by organization's Counsel's Office. Final approval by the PIO should define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized, the use of organizational email addresses on public social media sites is prohibited. In instances where users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the organization and staff. These expectations are outlined below.

a. Use of Social Media within the Scope of Official Duties
The PIO, or designee, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of the organization. However, PIO approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the IT infrastructure. In addition, PIO approval is not required for postings to private, organization approved social media collaboration sites (e.g., Yammer). Blanket approvals may be granted, as appropriate.

Accounts used to manage the organization's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow information security standards, be unique on each site, and must not be the same as passwords used to access other IT resources.

b. Guidelines for Personal Use of Social Media
Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache. Users should respect the privacy of the organization's staff and not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the organization."

Users should not use their personal social media accounts for official business, unless specifically authorized by the organization. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used on organizational devices and IT resources, to prevent unauthorized access to resources if the password is compromised.

# Secure Coding Practice Requirements

**Purpose**
Government organizations are under constant cyber-attacks that attempt to exploit vulnerabilities within computer systems and thereby threaten the confidentiality, integrity, and availability of information. A large number of vulnerabilities that are successfully exploited are due to software coding weaknesses and coding implementation flaws.

The objective of this coding standard is to ensure that code written is resilient to high-risk threats and to avoid the occurrence of the most common coding errors which create serious vulnerabilities in software.

While it is impossible to write code that is completely impervious to all possible attacks, implementing these coding standards throughout information systems will significantly reduce the risk of disclosure, alteration or destruction of information due to software vulnerabilities.

**Policy Statement**
All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.

The items enumerated in this standard are not an exhaustive list of high-risk attacks and common coding errors but rather a list of the most damaging and pervasive.

Therefore, code written must contain mitigating controls not only for the items specifically articulated in the standard below, but also for any medium and high-risk threats that are identified during a system's life cycle.

High risk threats include, but are not limited to:

1. Code Injection
2. Cross-site scripting (XSS)
3. Cross-site request forgery (CSRF)
4. Information leakage and improper error handling
5. Missing Authentication for Critical Function
6. Missing Encryption of Sensitive Data
7. URL Redirection to Untrusted Site ('Open Redirect')

At a minimum, code must eliminate or mitigate the threats identified in the current version of the Open Web Application Security Project (OWASP) Top 10 Most Critical Application Security Risks ('OWASP Top 10') and the Common Weakness Enumeration (CWE)/SANS Top 25 Most Dangerous Software Errors ('CWE/SANS Top 25') publications.

Both OWASP and CWE/SANS periodically reissue their respective lists based on changes in vulnerability and exploitation patterns.

Developers are required to independently remain aware of updates to these lists and incorporate any new recommendations.

Use of common security control libraries and common API's, that have undergone security testing, is required to ensure a consistent approach that minimizes defects and prevents exploitation. When available, publicly available or vendor-supplied libraries or APIs should be used unless there's a business case developed and exception granted by the Information Security Officer (ISO)/designated security representative to develop a custom library.

To prevent defects or detect and remove them early, thereby realizing significant cost and schedule benefits to the entity, code must be checked for errors throughout development and during maintenance.

Entities must verify that the software assurance model used by the vendor is in line with this standard through vendor assurances, security testing and/or contract requirements.

**Compliance**

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

# Personnel Cybersecurity Policy

**Personnel Security**

- The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific entity sensitive information not covered in the general security training.All security training must be reinforced at least annually and must be tracked by the entity.

- An entity must require its workforce to abide by the Acceptable Use of Information Technology Resources (2-G) Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

- All job positions must be evaluated by the HR to determine whether they require access to sensitive information and/or sensitive information technology assets.

- For those job positions requiring access to sensitive information and sensitive information technology assets, entities must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records.

The suitability determination must provide reasonable grounds for the entity to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the entity.

- A process must be established within the entity to repeat or review suitability determinations periodically and upon change of job duties or position.

# Inventory Policy

**Purpose**

- The purpose of this Policy is to protect and preserve Automotive Glass Experts' technology assets, and to ensure the confidentiality, integrity, and availability of Automotive Glass Experts's Information Systems, technological resources, and data.

- It is critically important for Automotive Glass Experts to know the location and status of all of its computers, devices, and other equipment that can be used to access Automotive Glass Experts's technology assets, Information Systems, and related resources. In order to do so, Automotive Glass Experts will maintain up-to-date inventory lists and asset controls. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols include documenting and supporting recovery and replacement of missing equipment and assets, including documenting and supporting insurance activities related to such equipment and assets. This Policy defines the responsibility of everyone within Automotive Glass Experts to ensure asset inventories are current and effective controls are in place to identify, track, manage, and dispose of assets properly.

**Policy Scope**

- This Policy covers all of Automotive Glass Experts's cybersecurity practices across all areas of its business. All Automotive Glass Experts employees, including contractors, third parties, Third Party Service Providers, and anyone else who is in possession of Automotive Glass Experts's equipment and/or assets, are required to comply with this Policy.

**Policy Statement**

**Asset Types**

Automotive Glass Experts will track all of its technology assets, including but not limited to:

- Desktop workstations
- Laptop mobile computers
- Tablet devices
- Software
- Printers, copiers, fax machines, and multifunction print devices
- Mobile handheld devices such as phones
- Scanners
- Servers
- Network devices (e.g., firewalls, routers, switches, un-interruptable power supplies, endpoint network hardware, and storage)
- External storage devices (including USB thumb drives)

# Hardware & Software Asset Policy

**Implementation**
Currently, the below requirements are fulfilled by the following:

- N/A

**IT Asset Management**

- All IT hardware and software assets must be assigned to a designated business unit or individual.

- Entities are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

- Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

**Asset Tracking Requirements**
Automotive Glass Experts will create an asset tracking database to track all of Automotive Glass Experts's assets, which will include categories such as:

- Type of asset (hardware such as computer, phone, tablet, and software)
- Make, model, serial number, and descriptor of asset
- Owner of asset
- Location of asset
- In active service or offline and stored

All information on an asset will be entered and maintained in the Automotive Glass Experts's asset tracking database before redeploying an asset. Automotive Glass Experts will own, be fully licensed, and be in full compliance with licensing entitlements of its software to minimize the risk of legal and regulatory problems. A process to identify unauthorized hardware and/or software will be undertaken periodically and, if any unauthorized hardware or software is discovered, immediate action will be taken to remedy the situation.

Automotive Glass Experts's asset tracking database will be reviewed periodically for accuracy and completeness.

**Asset Disposal and Repurposing**
Procedures for secure disposal or repurposing of equipment and resources will be established and implemented prior to reassignment, transfer, transport, or surplus.

Sensitive data will be removed prior to disposal of any asset. A data destruction protocol will be established and implemented for data destruction. Physical media that is storing confidential, sensitive, Nonpublic Information or Personally Identifiable Information will be destroyed if it is not being reused.

# Log Management Policy

**Definitions**

- End points: Any user device connected to a network. End points can include personal computers, personal digital assistants, scanners, etc.

- Flow: The traffic that corresponds to a logical connection between two processes in the network.

- IP: Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet.

- Packet: The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

**Overview**

Most components of the IT infrastructure at Automotive Glass Experts are capable of producing logs chronicling their activity over time. These logs often contain very detailed information about the activities of applications and the layers of software and hardware that support those applications. Logging from critical systems, applications, and services can provide key information and potential indicators of compromise and is critical to have for forensics analysis.

**Purpose**

Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance. Automotive Glass Experts will perform a periodic risk assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilization – how much capacity is used by services
- Security Events – what activity occurred during an incident, and when
- User Activity – what people are doing with services

## Policy Detail

**Log generation**

Depending on the volume of activity and the amount of information in each log entry, logs have the potential of being very large. Information in logs often cannot be controlled by application, system, or network administrators, so while the listed items are highly desirable, they should not be viewed as absolute requirements.

**Application logs**

Application logs identify what transactions have been performed, at what time, and for whom. Those logs may also describe the hardware and operating system resources that were used to execute that transaction.

**System logs**

System logs for operating systems and services, such as web, database, authentication, print, etc., provide detailed information about their activity and are an integral part of system administration.

When related to application logs, they provide an additional layer of detail that is not observable from the application itself. Service logs can also aid in intrusion analysis, when an intrusion bypasses the application itself.

Change management logs, that document changes in the IT or business environment, provide context for the automatically generated logs.

Other sources, such as physical access or surveillance logs, can provide context when investigating security incidents.

Client workstations also generate system logs that are of interest, particularly for local authentication, malware detection, and host-based firewalls.

**Network logs**

Network devices, such as firewalls, intrusion detection/prevention systems, routers, and switches are generally capable of logging information. These logs have value of their own to network administrators, but they also may be used to enhance the information in application and other logs.

Many components of the IT infrastructure, such as routers and network-based firewalls, generate logs. All of the logs have potential value and should be maintained. These logs typically describe flows of information through the network, but not the individual packets contained in that flow.

Other components for the network infrastructure, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers, provide valuable information about network configuration elements, such as IP addresses, that change over time.

**Time synchronization**
One of the important functions of a log management infrastructure is to relate records from various sources by time. Therefore, it is important that all components of the IT infrastructure have synchronized clocks. Automotive Glass Experts uses Network Time Protocol (NTP) for time synchronization.

**Use of log information**
Logs often contain information that, if misused, could represent an invasion of the privacy of members of Automotive Glass Experts. While it is necessary for Automotive Glass Experts to perform regular collection and monitoring of these logs, this activity should be done in the least invasive manner.

**Baseline behavior**
It is essential that a baseline of activity, within the IT infrastructure, be established and tracked as it changes over time. Understanding baseline behavior allows for the detection of anomalous behavior, which could indicate a security incident or a change in normal usage patterns. Procedures will be in place to ensure that this information is reviewed on a regular and timely basis.

**Investigation**
When an incident occurs, various ad hoc questions will need to be answered. These incidents may be security related, or they may be due to a malfunction, a change in the IT infrastructure, or a change in usage patterns.

Whatever the cause of the incident, it will be necessary to retrieve and report log records.

Thresholds shall be established that dictate what level of staff or management response is required for any given log entry or group of entries and detailed in a procedure.

**Log record life-cycle management**
When logs document or contain valuable information related to activities of Automotive Glass Experts's information resources or the people who manage those resources, they are Automotive Glass Experts Administrative Records, subject to the requirements of Automotive Glass Experts to ensure that they are appropriately managed and preserved and can be retrieved as needed.

**Retention**
To facilitate investigations, as well as to protect privacy, the retention of log records should be well defined to provide an appropriate balance among the following:

- Confidentiality of specific individuals' activities
- The need to support investigations
- The cost of retaining the records

Care should be taken not to retain log records that are not needed. The cost of long- term retention can be significant and could expose Automotive Glass Experts to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.

**Log management infrastructure**
A log management infrastructure will be established to provide common management of log records. To facilitate the creation of log management infrastructures, system-wide groups will be established to address the following issues:

- Technology solutions that can be used to build log management infrastructures

- Typical retention periods for common examples of logged information

# Classification Policy

**Overview**
The purpose of this policy is to classify information, data, and risk in order to enhance Automotive Glass Experts' awareness and understanding of the information and data we manage, as well as to be better prepared for potential cyber risks.

# Information Classification Policy

**Information Classification and Handling**

- All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.
- All information assets must have an information owner established within the lines of business.
- Information must be properly managed from its creation, through authorized use, to proper disposal.
- All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.
- An information asset must be classified based on the highest level necessitated by its individual data elements.
- If the entity is unable to determine the confidentiality classification of information or the information is personal identifying information (PII) the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
- Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- The entity must communicate the requirements for secure handling of information to its workforce.
- A written or electronic inventory of all information assets must be maintained.
- Content made available to the general public must be reviewed according to a process that will be defined and approved by the entity. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- PPI must not be made available without appropriate safeguards approved by the entity.

For non-public information to be released outside the entity or shared between other entities, a process must be established that, at a minimum:

a. evaluates and documents the sensitivity of the information to be released or shared;

b. identifies the responsibilities of each party for protecting the information;

c. defines the minimum controls required to transmit and use the information;

d. records the measures that each party has in place to protect the information;

e. defines a method for compliance measurement;

f. provides a signoff procedure for each party to accept responsibilities; and

g. establishes a schedule and procedure for reviewing the controls.

**Information Classification Scheme**
All information and/or information systems must be classified. Information classification is based on three principles of security:

1) confidentiality,
2) integrity, and
3) availability.

For each principle, information can be classified as low, moderate, or high. When classifying the impact, the entity should consider how the information or information systems are used to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Impact levels are defined as limited, serious, and severe or catastrophic. For the purposes of classification, limited impact shall be deemed to include no impact.

| Potential Impact | Definitions |
|---|---|
| Low | The potential impact is low if—The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| Medium | The potential impact is moderate if—The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.<br>A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries |
| High | The potential impact is high if—The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.<br>A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. |

Each entity should review the impact levels in the context of its own operational environment. Figure 2 shows the *Information Asset Classification Categories.*

| | INFORMATION CLASSIFICATION CATEGORIES per FIPS 199 | | |
|---|---|---|---|
| | Low | Medium | High |
| **Confidentiality**<br>Consider impact of unauthorized disclosure on factors such as:<br>• Health and Safety<br>• Financial Loss<br>• SE Mission/Programs<br>• Public Trust | The unauthorized disclosure of information could be expected to have limited or no impact on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious impact on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic impact on organizational operations, organizational assets, or individuals. |
| **Integrity**<br>Consider impact of unauthorized modification or destruction on factors such as:<br>• Health and Safety<br>• Financial Loss<br>• SE Mission/Programs<br>• Public Trust | The unauthorized modification or destruction of information could be expected to have limited or no impact on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious impact on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic impact on organizational operations, organizational assets, or individuals. |
| **Availability**<br>Consider impact of untimely or unreliable access to information on factors such as:<br>• Health and Safety<br>• Financial Loss<br>• SE Mission/Programs<br>▪ Public Trust | The disruption of access to or use of information or an Information System could be expected to have limited or no impact on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an Information System could be expected to have a serious impact on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an Information System could be expected to have a severe or catastrophic impact on organizational operations, organizational assets, or individuals. |

Figure 2: Information Asset Classification Matrix - *National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems*

**Information Classification Process**
The information classification process must include the following:

- Identification of information assets;
- Classification of information assets; by confidentiality, integrity, and availability ("CIA"); and
- Determining controls based upon the classification.

**1. Identification of Information Assets**

- Identification of information assets involves creating an inventory of all information assets in the entity. The following items need to be considered when constructing this inventory:

a. Grouping of information assets
b. Determining the information owner
c. Determining the information custodian
d. Identifying information assets

**A.Grouping of Information Assets**
To facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to appropriately group information assets together. A broad grouping may result in applying controls unnecessarily as the asset must be classified at the highest level necessitated by its individual data elements.For example, if a Human Resources unit decides to classify all of their personnel files as a single information asset and any one of those files contains a name and social security number, the entire grouping would need to be protected with moderate confidentiality controls.

A narrow grouping allows for more precise targeting of controls. However, as there are more information assets to classify, this increases the complexity of the classification and the management of controls.Using the previous example, classifying the multitude of personnel files (e.g., appointment letters, timecards, position classifications, holiday waivers) as individual information assets requires a different set of controls for each classification.

In the case of an information technology system, such as a database, data warehouse, or application server, while it may be easier to apply a single set of controls as a result of classifying the system as a single entity, costs may be reduced by applying the controls to the individual elements, such as specific fields, records, or applications. Therefore, it is important that the entity evaluates the risk and cost benefit of grouping a given set of assets.

**B. Determining the Information Owner**
Responsibility for the classification and definition of controls for an information asset belongs to an individual in a managerial position who is ultimately responsible for the confidentiality, integrity, and availability of that information. If multiple individuals are found to be "owners" of the same information asset, a single individual owner must be designated by a higher level of management. The information owner is responsible for determining the information's classification, how and by whom the information will be used.

Owners must understand the uses and risks associated with the information for which they are responsible and any laws, regulations, or policies which govern access and use. Each owner must exercise due diligence with respect to the proper classification of data in order to prevent improper disclosure and access.

**C.Determining the Information Custodian**
Information custodians are people, units, or organizations responsible for implementing the authorized controls for information assets based on the classification level. An information asset may have multiple custodians. Based on the information owner's requirements, the custodian secures the information, applying safeguards appropriate to the information's classification level. Information custodians can be from within the entity or from third parties (e.g., another entity). If the custodian is a third party, a formal, written agreement between the custodian's organization and the entity that owns the information must specify the responsibilities of each party. An information custodian may also be the information owner.

**D.Identifying Information Assets**
For each information asset in their control, the information owner must identify at a minimum:

- Source of the information asset (e.g., unit, agency)
- Use of the information asset (i.e., purpose/business function)
- Business processes dependent on the information asset
- Users/groups of users of the information asset

**2.Classification of Information Assets**
Owners must answer the questions in the Information Asset Classification Worksheet to determine the classification of their information assets. It is appropriate to recruit and work with subject matter experts who have specific knowledge about the information asset, such as Counsel's Office and the Records Management Officer. The Information Security Officer (ISO)/designated security representative may also be called upon to advise and assist the information owner in determining the classification. An entity may add more questions to the Information Asset Classification Worksheet but may not alter or remove the original questions.

Information assets are classified according to confidentiality, integrity, and availability. Each of these three principles of security is individually rated as low, moderate, or high. For example, an information asset may have a confidentiality level of "high", an integrity level of "moderate", and an availability level of "low" (i.e., HML).

Questions are categorized by confidentiality, integrity, and availability. Each question must be answered sequentially, to the best of the information owners' abilities.

# Information Security Policy

## General Policies

**Purpose**
The purpose of the Information Security Framework is:

- To establish an approach to information security.
- To detect and protect against the compromise of information security such as misuse of data (physical and electronic), networks, computer systems and applications.
- To protect the reputation of the company concerning its ethical and legal responsibilities.
- To observe the rights and protect the privacy of our customers.

Automotive Glass Experts is fully committed to ensuring the Confidentiality, Integrity and Availability of the data entrusted to us by our clients and partners.

**Information Security Policy**
Automotive Glass Experts recognises the disciplines of confidentiality, integrity and availability in Information Security Management are integral parts of its management function. The management of Automotive Glass Experts these as primary responsibilities and fundamental to the best business practice of adopting appropriate Information Security Controls.

Automotive Glass Experts Information Security policy seeks to operate to the highest standards continuously and to focus on continual improvement through annual review.

We will:

- Comply with all the applicable laws, regulations, and contractual obligations.
- Implement continual improvement initiatives, including risk assessment and risk treatment strategies, while making the best use of its management resources to better Information Security requirements.
- Communicate our Information Security objectives, and its performance in achieving these objectives, throughout the organization and to interested parties.
- Adopt an Information Security Management System comprising organizational policies and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers and interested parties who come into contact with its work.
- Work closely with our customers, business partners and suppliers in seeking to establish appropriate Information Security standards.
- Adopt a forward-looking view on future business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security.

- Train all members of staff in the needs and responsibilities of Information Security Management.

- Constantly strive to meet, and where possible exceed, our customer's, staff, and partners expectations.

**Organizational Security**
Information security requires both an information risk management function and an information technology security function. Depending on the structure of the entity, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high-level executive or a group that includes high level executives.

1. Each entity must designate an individual or group to be responsible for the risk management function assuring that:

a. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and

b. the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

2. Each entity must designate an individual or group to be responsible for the technical information security function.

For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer (ISO)/designated security representative. This function will be responsible for evaluating and advising on information security risks.

a.Information security risk decisions must be made through consultation with both function areas described in a. above.

b. Although the technical information security function may be outsourced to third parties, each entity retains overall responsibility for the security of the information that it owns.

**Functional Responsibilities**
Executive management is responsible for:

1. evaluating and accepting risk on behalf of the entity;

2. identifying information security responsibilities and goals and integrating them into relevant processes;

3. supporting the consistent implementation of information security policies and standards;

4. supporting security through clear direction and demonstrated commitment of appropriate resources;

5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated security representative;

6.implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;

7.implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;

8.determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;

9.participating in the response to security incidents;

10. complying with notification requirements in the event of a breach of private information;

11. adhering to specific legal and regulatory requirements related to information security;

12. communicating legal and regulatory requirements to the ISO/designated security representative; and

13. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

**The ISO/designated security representative is responsible for:**

1. maintaining familiarity with business functions and requirements;

2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;

3. assessing compliance with information security policies and legal and regulatory information security requirements; evaluating and understanding information security risks and how to appropriately manage those risks;

4. representing and assuring security architecture considerations are addressed; advising on security issues related to procurement of products and services;

5. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;

6.disseminating threat information to appropriate parties;

7. participating in the response to potential security incidents;

8. participating in the development of enterprise policies and standards that considers the entity's needs; and promoting information security awareness.

**IT management is responsible for:**
1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;

2. providing resources needed to maintain a level of information security control consistent with this policy;

3. identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;

4. implementing the proper controls for information owned based on the classification designations;

4. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);

5. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and

6.implementing business continuity and disaster recovery plans.

**The workforce is responsible for:**

- understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
- protecting information and resources from unauthorized use or disclosure;
- protecting personal, private, sensitive information from unauthorized use or disclosure;
- abiding by Acceptable Use of Information Technology Resources Policy
- reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.

**The CISO is responsible for:**

- providing in-house expertise as security consultants as needed;
- developing the security program and strategy, including measures of effectiveness;
- establishing and maintaining enterprise information security policy and standards;
- assessing compliance with security policies and standards;
- advising on secure system engineering;
- providing incident response coordination and expertise;

- monitoring networks for anomalies;
- monitoring external sources for indications of data breaches, defacements, etc.
- maintaining ongoing contact with security groups/associations and relevant authorities;
- providing timely notification of current threats and vulnerabilities; and
- providing awareness materials and training resources.

**Separation of Duties**

- To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
- Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.
- The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

**Information Risk Management**

- Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
- Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
- Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
- Risk assessment results, and the decisions made based on these results, must be documented.

**Account Management and Access Control**

- All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT).
- Except as described in the, Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.
- Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.

- Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

- Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.

- Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

- Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.

- Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).

- Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with entity missions and business functions (i.e., least privilege).

- Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

- Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored and the user should have no expectation of privacy.

- Advance approval for any remote access connection must be provided by the entity. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.

- All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.

- Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

*Associated Standards: Account Management/Access Control Standard; Authentication Tokens Standard; Remote Access Standard; Security Logging Standard*

**Systems Security**

a. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.

1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of the entity. A list of assigned individuals or groups must be centrally maintained.

2. Security must be considered at system inception and documented as part of the decision to create or modify a system.

3. All systems must be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).

4. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.

5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.

6.Environments and test plans must be established to validate the system works as intended prior to deployment in production.

7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).

8. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):

1. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.

2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.

3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:

i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or

ii. sensitive data is masked or overwritten with fictional information.

4. Where technically feasible, development software and tools must not be maintained on production systems.

5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.

6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.

7. Privileged access to production systems by development staff must be restricted.

8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:

1.Connections between systems must be authorized by the executive management of all relevant entities and protected by the implementation of appropriate controls.

2. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to assure:

i. the business case for the connection is still valid and the connection is still required; and

ii. the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.

3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:

i. Internet accessible systems and internal systems;

ii. systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and

iii. user and server segments.

4. Network management must be performed from a secure, dedicated network.

5.Authentication is required for all users connecting to internal systems.

6. Network authentication is required for all devices connecting to internal networks.

7. Only authorized individuals or business units may capture or monitor network traffic.

8. A risk assessment must be performed in consultation with the ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

*Associated Standards: Secure System Development Lifecycle Standard; Secure Coding Standard; Security Logging Standard; Secure Configuration Management Standard*

**Collaborative Computing Devices**

a.Collaborative computing devices must:

1. prohibit remote activation; and
2. provide users physically present at the devices with an explicit indication of use.
3. Must provide simple methods to physically disconnect collaborative computing devices.

**Vulnerability Management**

a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

b. All systems are subject to periodic penetration testing.

c.Penetration tests are required periodically for all critical environments/systems.

d. Where the entity has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated.

e.Scanning/testing and mitigation must be included in third party agreements.

f. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk.

g.Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

i. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

*Associated Standards: Patch Management Standard; Vulnerability Scanning Standard*

**Operations Security**

a. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.

b. System configurations must follow approved configuration standards.

c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

d. Where the entity provides a server, application or network service to another entity, operational and management responsibilities must be coordinated by all impacted entities.

e. Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed

f. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.

g. Controls must be implemented to disable automatic execution of content from removable media.

h. Controls must be implemented to limit storage of information to authorized locations.

i. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.

j. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

k. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

l. Systems which can no longer be supported or patched to current versions must be removed.

m. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and record events to provide evidence and to reconstruct lost or damaged data.

n. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements.

o. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic.

p. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

q.Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. At a s

1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

r. Backup copies of entity information, software, and system images must be taken regularly in accordance with the entity's defined requirements.

s. Backups and restoration must be tested regularly.Separation of duties must be applied to these functions.

t. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

*Associated Standards*: *Secure Configuration Management Standard; Security Logging Standard; Cyber Incident Response Standard; Account Management/Access Control Standard*

# Identity and Access Management Policy

Account management and access control includes the process of requesting, creating, issuing, modifying and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions.

**Account Management/Access Control Roles**

Account management and access control require that the roles of Information Owner, Account Manager and, optionally, Account Administrator and Entitlement Administrator, are defined and assigned for each resource and application. A listing of authorized users in these roles must be documented and maintained. The associated tasks and responsibilities for each role are described below. Each role may belong to one or more individuals depending on the application.In some cases, a single individual or group may be assigned more than one of these roles.

a. Information Owner: Information owners are people at the managerial level within an entity who:

1.Delegate account managers to ensure the appropriate level of information access is provided. Delegation can be to individual users, groups and/or third parties (e.g., another entity).

2.Define roles and groups, as well as the corresponding level of access to resources for that role or group.

3.Determining who should have access.

4.Determine the identity assurance level for the application and/or data.

5.Review that accounts and access controls are commensurate with overall business function and that the associated rights have been properly assigned, at a minimum, annually.

6.Require business units with access to protected resources to notify account managers when accounts are no longer required, such as when users are terminated or transferred and when individual access requirements change.

b. Account Manager: Account managers maintain accounts. They are the delegated custodians of protected data. Account managers:

1.Maintain appropriate levels of communication with the information owners to determine the level or degree of access granted to an individual.

2.Determine the technical specifications needed to set access privileges.

3.Delegate account management functions to account administrators.

4.Create and maintain procedures used in managing accounts.

5.Perform all account administrator duties as required.

c. Account Administrators: Account administrators are an optional subset of the account manager role.They do not determine procedures. System rights and/or responsibilities are assigned to them by the account manager.All account administrator responsibilities are contained within the role of account manager should an account administrator not exist. A subset of account administrator duties may be assigned as appropriate. For example, a role for password reset only may exist for service desk employees. Additionally, some of these responsibilities may remain with the account manager should that manager determine it is necessary. For account management, the administrator may:

1.Maintain any necessary information supporting account administration activities, including account management requests and approvals.

2.Enroll new users.

3.Enable/disable user accounts.

4.Create and maintain user roles and groups.

5.Assign rights and privileges to a user or group.

6.Collect data to periodically review user accounts and their associated rights.

7.Assign new authentication tokens (e.g., password resets).

d. Entitlement Administrator
Entitlement administrators are an optional subset of the account manager role.Rights and/or responsibilities are assigned to them by the information owner and generally include:
1.Assign rights and privileges to a user or group.

2.Collect data to periodically review user accounts and their associated rights.

3.Maintain any necessary information supporting account administration activities including account management requests and approvals.

**Account Types**
Account types include: Individual, Privileged, Service, Shared, Default Non-Privileged (e.g., Guest, Anonymous), Emergency, and Temporary. All account types must adhere to all applicable rules as defined in the Authentication Tokens Standard.

a. Individual Accounts: An individual account is a unique account issued to a single user. The account enables the user to authenticate to systems with a digital identity. After a user is authenticated, the user is authorized or denied access to the system based on the permissions that are assigned directly or indirectly to that user.

b. Privileged Accounts: A privileged account is an account which provides increased access and requires additional authorization. Examples include a network, system or security administrator account. A privileged account may only be provided to members of the workforce whom require it to accomplish their job duties. The use of privileged accounts must be compliant with the principle of least privilege. Access will be restricted to only those programs or processes specifically needed to perform authorized business tasks and no more. There are two privileged account types - Administrative Accounts and Default Accounts.

- Administrative Accounts

Accounts given to a user that allow the right to modify the operating system or platform settings, or those which allow modifications to other accounts. These accounts must:

1. be at an Identity Assurance Level commensurate with the protected resources to which they access.

2. not have user-IDs that give any indication of the user's privilege level, e.g., supervisor, manager, administrator, or any flavor thereof.

3. be internally identifiable as an administrative account per a standardized naming convention.

4. be revoked in accordance with organizational requirements

- Default Privileged Accounts

Default privileged accounts (e.g., root, Administrator) are provided with a particular system and cannot be removed without affecting the functionality of the system. Default privileged accounts must:

1. be disabled if not in use or renamed if technically possible.

2. only be used for the initial system installation or as a service account. When technically feasible, alerts must be issued to the appropriate personnel when there is an attempt to log-in with the account for access.

3. not use the initial default password provided with the system.

4. have password known or accessible by at least two individuals within the SE, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

c. Service Accounts: A service account is not intended to be given to a user but is provided for a process. It is to be used in situations such as to allow a system to run jobs and services independent of user interaction. Service accounts must:

1. have an assigned owner responsible for documenting and managing the account.

2. be restricted to specific devices and hours when possible.

3. never be used interactively by a user for any purpose other than the initial system installation or if absolutely required for system troubleshooting or maintenance. Wherever technically feasible, administrators should leverage “switch user” (SU) or “run as” for executing processes as service accounts.

4. never be for any purpose beyond their initial scope.

5. be internally identifiable as a service account per a standardized naming convention, where possible.

6. not allow its password to be reset according to any standardized and/or forced schedule. However, should an employee with knowledge of said password leave the entity, that password must be changed immediately.

7. have password known or accessible by at least two individuals within the entity, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

d. Shared Accounts: A shared account is any account where more than one person knows the password and/or uses the same authentication token. Use of shared accounts is only allowed when there is a system or business limitation preventing use of individual accounts. These cases must be documented by the information owner and reviewed by the Information Security Officer (ISO)/designated security representative. Additional compensatory controls must be implemented to confirm accountability is maintained. Shared accounts must:

1.have the tokens (e.g. password) reset when any of its users no longer needs access, or otherwise in accordance with the Authentication Tokens Standard.

2.be restricted to specific devices and hours when possible.

3.wherever technically feasible, have its users log on to the system with their individual accounts and “switch user” (SU) or “run as” the shared account.

4.have strictly limited permissions and access only to the system(s) required.

e. Default Non-Privileged Accounts: The default non-privileged account (guest or anonymous user) is an account for people who do not have individual accounts. An example of where this might be necessary is on a public Wi-Fi network. This account type must:

1.be disabled until necessary.

2.have limited rights and permissions.

3.only be allowed after a risk assessment

4.have compensatory controls that include restricted network access.

5.be assigned a password that the user cannot change but that is changed monthly, at a minimum, by an administrator.

6.not allow the account to be assigned for delegation by another account.

7.have a log maintained of users to whom the password is given.

f. Emergency Accounts: Emergency Accounts are intended for short-term use and include restrictions on creation, point of origin, and usage (i.e., time of day, day of week). SEs may establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency accounts must be automatically disabled after 24 hours.

g. Temporary Accounts: Temporary accounts are intended for short-term use and include restrictions on creation, point of origin, usage (i.e., time of day, day of week), and must have start and stop dates. An entity may establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation, such as for vendors, manufacturers, etc. These accounts must have strictly limited permissions and access only to the systems required.

**Account Management and Access Control Functions**

Automated mechanisms must be employed to monitor the use and management of accounts. These mechanisms must allow for usage monitoring and notification of atypical account usage. Thresholds for alerting should be set based on the criticality of the system or assurance level of the account.

Staff in the appropriate account management/access control role(s) must be notified when account management activities occur, such as, accounts are no longer required, users are terminated or transferred, or system usage or need-to-know changes. This should be automated where technically possible.

Automated access control policies that enforce approved authorizations for information and system resources must be in place within systems. These access control polices could be identity, role or attribute based.

By default, no one has access unless authorized.

The Identity Assurance Level (IAL) of a system determines the degree of certainty required when proofing the identity of a user. The following table describes the level of confidence associated with each IAL.

| Identity Assurance Level | Description |
|---|---|
| 1 | Low or no confidence in the asserted identity's validity |
| 2 | Confidence in the asserted identity's validity |
| 3 | High confidence in the asserted identity's validity |

Table 1 reflects the standards for account management at each assurance level.

Table 1 – Account Management Standards per Identity Assurance Level

| | Identity Assurance Levels | | |
|---|---|---|---|
| Category | 1 | 2 | 2 |
| Account disabled automatically after x days of inactivity | 1096 | 90 | 90 |
| Send notification x days before account disabled | 30 | 30 | 14 |
| Account locked after x number of consecutive failed login attempts | 10 | 5 | 3 |
| Account creation requires an authoritative attribute that ties the user to their account. For example, this could be an employee ID, driver's license ID, tax ID, or unique individual email address. | No | Yes | Yes |
| Email notification will be sent to the user for the following events:<br>• Token change (password, pre-registered knowledge token, out of band (OOB) token information)<br>• Account disabled due to invalid attempts<br>• Forgotten User Identification (UID) issued<br>• Account attribute change (e.g., name change)<br>• Account re-activation | If known | Yes | Yes |
| Self-service functionality allowed | Yes | Yes | No |

For all Assurance Levels, the following must be adhered to.

**a. Creating New Accounts:** To create an account, there must be a valid access authorization based on an approved business justification and a request must be made to create the account.

**b. Modifying Account Attributes (i.e., changing users' names, demographics, etc.):** Modifications must only be made by the authenticated user or an authorized account manager.

**c. Enabling Access**: Access is granted, based on the principle of least privilege, with a valid access authorization.

**d. Modifying Access:** Access modifications must include a valid authorization. When there is a position change (not including separation), access is immediately reviewed and removed when no longer needed.

**e. Disabling Accounts/Removing Access:**

- Event/Risk Based (Administrative Disable): When an account poses or has the potential to pose a significant risk, either the account is disabled and/or access attributes are removed upon discovery of the risk. Close coordination between the information owners, account managers/administrators, legal, incident response stakeholders and human resource managers is essential in order for timely execution of removing or restricting user access. Significant risk may include a disgruntled employee, or one who has been identified by as a potential risk. Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations. An account identifier is required to identify these accounts and prevent inappropriate re-enabling of the account/access. Re-enabling the account requires explicit approval of the entity, Self-service mechanisms may not be used to re-enable the account.

- De-provisioning Upon Separation: All user accounts (including privileged) must be disabled immediately upon separation. In addition, credentials must be revoked in accordance with organizational requirements, and access attributes must be removed. Self-service mechanisms may not be used to re-enable the account.

- Inactivity Disable: When an account is disabled due to inactivity, access attributes may remain unchanged if deemed appropriate by the information owner.

**f. Reviewing Accounts and Access:**

- Information owners must review all accounts on an annual basis (minimally) to determine if they are still needed.

- Access to privileged accounts must be reviewed every six months (minimally) to determine whether or not they are still needed.

- Information owners must review account authorizations and/or user access assignments on an annual basis (minimally) to determine if all access is still needed.

- Accounts or records of the account must be archived after 5 years of inactivity or after specific audit purposes are met.

**g. Unlocking User Accounts**: In order for an administrator or user support agent to unlock an account for a user, the user must be vetted through pre-registered knowledge tokens as per the Authentication Tokens Standard.

**h. Secure Log on Procedures:** Where technically feasible, access must be controlled by secure log-on procedures as follows:

- Must not display tokens (e.g., password, PIN) being entered.

- Must display the following information on completion of a successful log-on:
  1. Date and time of the previous successful log-on; and
  2. Details of any unsuccessful log-on attempts since the last successful log-on.

i. Session Inactivity Lock: Sessions must be locked after a maximum inactivity period of 15 minutes.Session inactivity locks are temporary actions taken when users stop work and move away from their immediate vicinity but do not want to log out because of the temporary nature of their absences. Users must re-authenticate to unlock the session.

**j. Connection Time-out:** Sessions must be automatically terminated after 18 hours or after “pre-defined” conditions such as targeted responses to certain types of incidents.

**k. Logging/Auditing/Monitoring:** All account activity must be logged and audited in accordance with the Security Logging Standard. The ability to modify or delete audit records must be limited to a subset of privileged accounts. Any modification to access attributes must be recorded and traceable to a single individual.

# Minimum Access Policy
## Password Policy

**Overview**
Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Automotive Glass Experts resources. All users, including contractors and vendors with access to Automotive Glass Experts systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

**Scope**
All employees, contractors, consultants, temporary and other workers at Automotive Glass Experts including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Automotive Glass Experts, or to devices or services that connect to a Automotive Glass Experts network or reside at a Company Site.

### Policy Statement

**1. Password Creation**

- All user-level and system-level passwords must conform to the "Password Construction Guidelines" set out in clause 2.5 of this document.
- Users should not use the same password for Automotive Glass Experts accounts as for other personal or other access (for example, personal ISP account, Internet Banking, social media accounts, etc.).
- Where possible, users should not re-use the same password for various Automotive Glass Experts access needs.

**2. Password Change**

- All user-level passwords must be changed at least every sixty calendar days.
- Password cracking or guessing may be performed on a periodic or random basis by the Automotive Glass Experts IT Team or Automotive Glass Experts security team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to comply with this policy.

**3. Password Protection**

- Refrain from sending plaintext passwords over networks or email, it could compromise security. Passwords sent in plain text can be read by anyone.
- Passwords must not be shared with anyone. All passwords are to be treated as restricted Automotive Glass Experts information.
- Passwords may be inserted into email messages, Alliance cases or other forms of electronic communication, but must be encrypted and the encryption key must be shared via a different media source. Refer to the Acceptable Encryption Policy.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share Automotive Glass Experts passwords with anyone, including administrative assistants, secretaries, managers, co-workers, and family members.

- Do not write passwords down and store them anywhere in your workspace.
- Do not store passwords in a file on a computer system or mobile devices (phone, tablet)
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident to the Automotive Glass Experts IT department immediately and request a change of passwords on all user access accounts.
- Password managers can be used, users must refer to the pre-authorised software list, held by InfoSec and IT departments.

**4. Application Development**

Application developers must ensure that their programs contain the following security precautions:

- Applications must support the authentication of individual users.
- Applications that authenticate against Active directory must authenticate against a dedicated Active Directory security group.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

**5. Password Construction Guidelines**

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks".

A good passphrase is relatively long and contains a combination of upper and lowercase letters, numeric and punctuation characters.

Passwords that are listed in the password blacklist will not be available for use.

Automotive Glass Experts Passwords must meet three of the four characteristics below:

- Contain at least 12 alphanumeric characters.
- Contain both upper- and lower-case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,$%^&*()_+|~-=\`{}[]:";'<>?,/).

**6. Password Examples**
BAD Examples

A password containing a single dictionary word (for example, Password).

- Contains personal information (for Example, Birth Date, Birth Year, Family Names, Pet Names).
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain a common word spelled backwards, preceded, or followed by a number (for example, terces, secret1 or 1secret).
- Some variation of "Welcome123" "Password123" "Changeme123

**7. Administrator Enforced Policies**
All Automotive Glass Experts systems administrators are responsible for ensuring that the network environment and all Operating Systems within the Company network are configured to support this password policy. The following configuration settings must be applied to all Active Directory Forests, Active Directory Domains, Windows member servers and Non-Windows servers which operate within any of the Company owned networks.

- Enforce Password History – This must be set to 10 passwords remembered, i.e.: The user may not be able to use his/her previous 10 passwords.
- Maximum Password Age – This must be set to 60 calendar days, so that the system enforces the change of the user's password every 60 calendar days.
- Minimum Password Age – This must be set to 10 calendar days, so that users can only change their passwords at will every 10 calendar days.
- Minimum Password Length – This must be set to 12 characters.
- Password Complexity – Must be enabled to ensure that passwords are case sensitive, alpha-numeric and contain special characters.
- Account Lockout Duration – Lockout duration should be set to 30 minutes.
- Account Lockout Threshold – Lockout Threshold should be set to 5 bad consecutive password attempts.
- Reset Account Lockout Counter – Reset Account Lockout Counter should be set to 30 minutes.
- IT Administrators need to update the password blacklist annually. The blacklist needs to be recorded, approved, and communicated by the IT manager.

**8. SuperUser / Administrator Passwords**
A Super User / Administrator account is a highly sensitive account and extreme caution should be taken when dealing with these accounts.

- Superuser or Administrator passwords should never be shared with anyone inside or outside the organization.

- All Administrators will be issued with a named Administrator account. Named administrator accounts will reflect the name of the person responsible for that specific account. The user will be responsible for their Administrator account and the safekeeping of the account password.

- All Administrators will be held responsible for the activities on their set account.

- All Administrator accounts must be enrolled, if supported by the system, with MFA Multi-Factor Authentication, the preference of the MFA options is, in order:

a. Authentication App
b.Phone Call
c.Alternate Email address
d.SMS

**9. Default Administrator Passwords**

- The default Administrator account usernames must be changed, where possible.

- The default Administrator account password must be changed during the implementation of the system.

- The passwords for the default administrator account should only be accessible to authorized personnel.

- Passwords for Default Administrator accounts will be changed annually and must be documented within the Access control framework document and stored in a secure location, this document should not be saved on any system within the company network.

- Passwords for default Administrator accounts should comply with the below rules, where applicable:

a. Minimum Password Length – This must be set to 20 characters.

b. Password Complexity – Must be enabled to ensure that passwords are case sensitive, alpha-numeric and contain special characters.

**10.Local Administrator Passwords**
The "Local Administrator Password Solution" (LAPS) provides the management of local account passwords of domain-joined computers. Passwords are stored in Active Directory and protected by ACL, so only eligible users can read it or request its reset.

- Users who are eligible to read the local administrator passwords are responsible for the safekeeping of the passwords.
- Local Administrator passwords must not be shared with any unauthorized person.
- Local Administrator passwords must be changed every 90 days.
- LAPS must be enrolled on all domain-joined devices.

**11.Mobile Phone Passwords**
Mobile phones that are used to access company information must comply with the Minimum Access Policy and must have a password set and must comply with the below:

- Minimum Password Length – This must be set to 5 characters.
- Password Complexity – Complex numeric, repeated, or consecutive numbers, such as "1111" or "1234", aren't allowed.
- Maximum minutes of inactivity before a password is required – 5 minutes.

**12.Password Managers**
The use of password managers has become more common, and the use of password managers is accepted within the environment, but must comply with the following:

- Password Managers need to be enrolled with your company-issued email address.
- Storing company passwords on a Password Managers enrolled with a personal email address is strictly prohibited.
- Multi-factor authentication must be enabled on the account.
- These accounts should never be shared with other internal or external parties.
- Individual Passwords may be shared through the Password Manager application and must be controlled through the Password Manager Application.
- Shared Passwords must be reviewed on a regular basis.
- The use of a password generator is allowed, but the password must meet the password requirements specified in section 2.5 of this document.

# Server Policy

## Introduction

**Overview**

Unsecured and vulnerable servers continue to be a major entry point for malicious threats. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

**Scope**

All employees, contractors, consultants, temporary and other workers at the company and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by the company or registered under a company -owned internal network domain.

This policy specifies requirements for equipment on the corporate company network.

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by the company. Effective implementation of this policy will minimize unauthorized access to the company Confidential information and technology.

**Policy Statement**

- General Requirements

All internal servers deployed at Automotive Glass Experts must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained, based on business needs, and approved by IT and Security

- The following items must be met:

Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

a. Server contact(s) and location, and a backup contact
b. Hardware and Operating System/Version
c. Main functions and applications, if applicable
d. Information in the corporate enterprise management system must be kept up to date.

- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

**Configuration Requirements**

- Operating System configuration should be in accordance with Server Hardening Procedure.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

- Passwords for any systems installed on the Server needs to comply with the Password Policy.

- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

- Servers should be physically located in an access-controlled environment.

- Servers are specifically prohibited from operating from uncontrolled areas.

**Monitoring**

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

a. All security related logs will be kept online for a minimum of 1 week.
b. Incremental backups will be retained for at least 1 month.
c. Weekly full backups of logs will be retained for at least 1 month.

- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

•Port-scan attacks

•Evidence of unauthorized access to privileged accounts

•Anomalous occurrences that are not related to specific applications on the host.

**References**

| **Document Name** |
| --- |
| Server Hardening Procedure |
| Password Policy |
| Exceptions Policy |

**Outputs**
The following records need to be kept and stored securely.

| Record | Responsable Person | Retention | Disposition |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

# Cloud Policy

**Overview**
Cloud computing would allow Automotive Glass Experts to take advantage of technologies for storing and/or sharing documents and other files, and virtual on-demand computing resources. Cloud computing can be beneficial in reducing cost and providing flexibility and scalability.

**Purpose**
The purpose of this policy is to ensure that Automotive Glass Experts can potentially make appropriate cloud adoption decisions and at the same time does not use, or allow the use of, inappropriate cloud service practices. Acceptable and unacceptable cloud adoption examples are listed in this policy. All other cloud use cases are approved on a case-by-case basis.

**Policy Detail**
It is the policy of Automotive Glass Experts to protect the confidentiality, security, and integrity of each member's non-public personal information. Automotive Glass Experts will take responsibility for its use of cloud computing services to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of Automotive Glass Experts.

This policy acknowledges the potential use of diligently vetted cloud services, only with:

- Providers who prove, and can document in writing, that they can provide appropriate levels of protection to Automotive Glass Experts data in categories that include, but are not limited to, transport, storage, encryption, backup, recovery, encryption key management, legal and regulatory jurisdiction, audit, or privacy

- Explicit procedures for all handling of Automotive Glass Experts information regardless of the storage, sharing or computing resource schemes

**Cloud Computing Services**
The category of cloud service offered by the provider has a significant impact on the split of responsibilities between the customer and the provider to manage security and associated risks.

- Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. The provider is supplying and responsible for securing basic IT resources such as machines, disks, and networks. The customer is responsible for the operating system and the entire software stack necessary to run applications and is responsible for the customer data placed into the cloud computing environment. This means most of the responsibility for securing the applications and the data falls onto the customer.

- Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. The infrastructure, software, and data are primarily the responsibility of the provider, since the customer has little control over any of these features. These aspects need appropriate handling in the contract and the Service Level Agreement (SLA).

- Platform as a Service (PaaS) is a cloud computing service that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Responsibility is likely shared between the customer and provider.

**Privacy Concerns**
There are information security and data privacy concerns about use of cloud computing services at Automotive Glass Experts. They include:

- Automotive Glass Experts may be limited in its protection or control of its data, potentially leading to a loss of security, lessened security, inability to comply with various regulations and data handling protection laws, or loss of privacy of data due to aggregation with data from other cloud consumers.

- Automotive Glass Experts's dependency on a third party for critical infrastructure and data handling processes.

- Automotive Glass Experts may have limited SLAs for a given provider's services and the third parties that a cloud vendor might contract with.

- Automotive Glass Experts is reliant on vendors' services for the security of the computing infrastructure.

**Diligence**
In evaluating the potential use of a particular cloud platform, Automotive Glass Experts will pay particular attention to the foregoing, and other privacy concerns, in addition to its documented vendor due diligence program.

**Exit Strategy**
Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. Automotive Glass Experts must determine how data would be recovered from the vendor.

**Examples**
The following table outlines the data classifications and proper handling of Automotive Glass Experts data.

| Data Classification | Public Cloud Computing, Storage or Sharing* | Private Cloud and On-premise Computing or Storage<br><br>User access restricted by username and password or another authentication |
|---|---|---|
| Financial Information | Not Allowed | Allowed<br>No special requirements, subject to any applicable laws |
| Intellectual Property | Allowed but Not Advised | Allowed<br>No special requirements, subject to any applicable laws |
| Other Non-Public Data | Allowed but Not Advised | Allowed<br>No special requirements, subject to any applicable laws |
| Other Public Data | Allowed | Allowed No special requirements, subject to any applicable laws |
| Personally Identifiable Information (PII) | Not Allowed | Allowed<br>No special requirements, subject to any applicable laws |

*See Policy 20 Cloud Computing Adoption Appendix A for approved and non- approved services.

# Appendix A

**Cloud Computing Adoption**
**Rev. April 01, 2021**

Approved Public Cloud Services
This listing is not represented to be exhaustive and is meant to serve as a point-in-time list of approved or disapproved public cloud services as of the revision date in this appendix. Any cloud service not explicitly listed as approved should be assumed to be not approved until documented otherwise.

| Services Approved for Automotive Glass Experts Use | Services Not Approved for Automotive Glass Experts Use |
|---|---|
| Amazon AWS | |
| MongoDB | |
| InfluxDB | |
| G-Suite/ Google Cloud & Drive | |
| | |
| | |

**Limited by user and intended use. See restrictions on data classification use in the main policy body*
***Approval under review as of the date of this revision*

# Wifi Policy

**Purpose**
The purpose of this policy is to secure and protect the information assets owned by Automotive Glass Experts Glass Services and to establish awareness and safe practices for connecting to free and unsecured Wi-Fi, and that which may be provided by Automotive Glass Experts Glass Services. Automotive Glass Experts provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Automotive Glass Experts grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

**Policy Detail**
Automotive Glass Experts Wi-Fi Network
The Automotive Glass Experts Wi-Fi network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it. For employee business use, it is designed to be a supplement to, and not a substitute for, the production wired local area network. For non-employees, it is also provided as a convenience, primarily as a way for members to access Automotive Glass Experts online products and services. Staff may easily demonstrate Automotive Glass Experts online products and services to members or prospects. Wi-Fi access points, located at the Head Office and in most branch offices, allow for compatible wireless device connectivity.

Microwaves, cordless telephones, neighboring APs, and other Radio Frequency (RF) devices that operate on the same frequencies as Wi-Fi, as well as physical infrastructure and/or barriers, are known sources of Wi-Fi signal interference. Wi-Fi bandwidth is shared by everyone connected to a given Wi-Fi access point (AP). As the number of Wi-Fi connections increase, the bandwidth available to each connection decreases and performance deteriorates. Therefore, the number and placement of APs in a given building is a considered design decision. Due to many variables out of direct Automotive Glass Experts control, availability, bandwidth, and access is not guaranteed.

The Automotive Glass Experts Wi-Fi network and connection to the Internet shall be:

- Secured with a passphrase and encryption, in accordance with current industry practice.
- Passphrases will be of appropriate complexity and changed at appropriate intervals, balancing security practice with the intended convenient business use of the Wi-Fi.
- Physically or logically separate from the Automotive Glass Experts production wired local area network (LAN) and its resources.
- Provided as a convenience for the use of Automotive Glass Experts employees, their vendors while visiting Automotive Glass Experts, the members of Automotive Glass Experts, and other visitors with Automotive Glass Experts's express permission via provision of an appropriate passphrase provided by their manager.

- Optionally provided to members and qualifying visitors, by Automotive Glass Experts's authorized staff, with the provision of an appropriate passphrase and may be accessed only with the agreement to acceptable use policy statements provided online or in a written or verbal format

- Accessed by employees only in accordance with the Acceptable Use policy and its cross-referenced policies seen in Policy 1 in this document

- Used for access to the Automotive Glass Experts production LAN only for business use and with the approved use of a Automotive Glass Experts issued virtual private network (VPN) connection. Passphrase to be approved/confirmed by IT.

Automotive Glass Experts's Wi-Fi service may be changed, the passphrase re-issued or rescinded, the network made unavailable, or otherwise removed without notice for the security or sustainability of Automotive Glass Experts business

**Personnel Security**

- The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific entity sensitive information not covered in the general security training.All security training must be reinforced at least annually and must be tracked by the entity.

- An entity must require its workforce to abide by the Acceptable Use of Information Technology Resources (2-G) Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

- All job positions must be evaluated by the HR[1] to determine whether they require access to sensitive information and/or sensitive information technology assets.

- For those job positions requiring access to sensitive information and sensitive information technology assets, entities must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the entity to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the entity.

- A process must be established within the entity to repeat or review suitability determinations periodically and upon change of job duties or position.

- Entities are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

When using Wi-Fi on a mobile device in a public establishment, there are precautions that should be followed.

Do:

- As with any Internet-connected device, defend your laptop, tablet, phone, etc. against Internet threats. Make sure your computer or device has the latest antivirus software, turn on the firewall, never perform a download on a public Internet connection, and use strong passwords.

- Look around before selecting a place to sit, consider a seat with your back to a wall and position your device so that someone nearby cannot easily see the screen.

- Assume all Wi-Fi links are suspicious, so choose a connection carefully. A rogue wireless link may have been set up by a hacker. Actively choose the one that is known to be the network you expect and have reason to trust.

- Try to confirm that a given Wi-Fi link is legitimate. Check the security level of the network by choosing the most secure connection, even if you have to pay for access. A password-protected connection (one that is unique for your use) is better than one with a widely shared passphrase and infinitely better than one without a passphrase.

- Consider that one of two similar-appearing SSIDs or connection names may be rogue and could have been setup by a hacker. Inquire of the manager of the establishment for information about their official Wi-Fi access point.

- Avoid free Wi-Fi with no encryption. Even if your website or other activity is using https (with a lock symbol in your browser) or other secure protocols, you are at much greater risk of snooping, eavesdropping, and hacking when on an open Wi- Fi connection (such as at the Airport, McDonald's, some hotels, etc.).

- Seek out Wi-Fi connections that use current industry accepted encryption methods and that generally will require the obtaining of a passphrase from the establishment.

- Consider using your cell phone data plan for sensitive activities rather than untrusted Wi-Fi, or your own mobile hotspot if you have one or have been provided with one.

- If you must use an open Wi-Fi, do not engage in high-risk transactions or highly-confidential communication without first connecting to a virtual private network (VPN).

- If sensitive information absolutely must be entered while using a public network, limit your activity and make sure that, at a minimum, your web browser connection is encrypted with the locked padlock icon visible in the corner of the browser window, and make sure the web address begins with https://. If possible, save your financial transactions for when you are on a trusted and secured connection, at home, for instance. Passwords, credit card numbers, online banking logins, and other financial information is less secure on a public network.

- Avoid visiting sites that can make it easier or more tempting for hackers to steal your data (for example, banking, social media, and any site where your credit card information is stored).

- If you need to connect to the Automotive Glass Experts network and are authorized to do so, choose a trusted and encrypted Wi-Fi AP, or use your personal hotspot. In every case, you must use your Automotive Glass Experts provided VPN at all times. The VPN tunnel encrypts your information and communications and besides, hackers are much less likely to be able to penetrate this tunnel and will prefer to seek less secure targets.

- In general, turn off your wireless network on your computer, tablet, or phone when you are not using it to prevent automatic connection to open and possibly dangerous APs. Set your device to not connect automatically to public or unknown and untrusted networks.

Do Not:

- Leave your device unattended, not even for a moment. Your device may be subject to loss or theft, and even if it is still where you left it, a thief could have installed a keylogger to capture your keystrokes or other malware to monitor or intercept the device or connection.

- Email or originate other messages of a confidential nature or conduct banking or other sensitive activities, and definitely not when connected to an open, unencrypted Wi-Fi.

- Allow automatic connection to or connection to first Wi-Fi AP your device finds, as it may be a rogue AP set up by a thief. Rather, choose the one that is known to be the network you expect and have reason to trust.

# Firewall Policy

**Overview**
Automotive Glass Experts operates network firewalls between the Internet and its private internal network to create a secure operating environment for Automotive Glass Experts's computer and network resources. A firewall is just one element of a layered approach to network security.

**Purpose**
This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to Automotive Glass Experts's network and information systems.

The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks
- Block unwanted traffic as determined by the firewall ruleset
- Hide vulnerable internal systems from the Internet
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet
- Log traffic to and from the internal network
- Provide robust authentication
- Provide virtual private network (VPN) connectivity

**Policy Detail**
All network firewalls, installed and implemented, must conform to the current standards as determined by Automotive Glass Experts's IT Department. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this policy.

- Outbound – allows all Internet traffic to authorized groups
- All traffic is authorized by Internet Protocol (IP) address and port The firewalls will provide:

a. Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.

b. Application proxy – every packet is stopped at the proxy firewall and examined and compared to the rules configured into the firewall.

c. Stateful Inspection – a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

The firewalls will protect against:

- IP spoofing attacks – the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
- Denial-of-Service (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets.
- Any network information utility that would reveal information about the Automotive Glass Experts domain.

A change control process is required before any firewall rules are modified. Prior to implementation, the Third Party Vendor and Automotive Glass Experts network administrators are required to have the modifications approved by the Director of IT or the Director of IT. All related documentation is to be retained for three (3) years.

All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.

Firewall rulesets and configurations require periodic review to ensure they afford the required levels of protection:

- Automotive Glass Experts must review all network firewall rulesets and configurations during the initial implementation process and periodically thereafter.
- Firewall rulesets and configurations must be backed up frequently to alternate storage (not on the same device).

Multiple generations must be captured and retained, to preserve the integrity of the data, should restoration be required.

- Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

**Responsibilities**

The IT Department is responsible for implementing and maintaining Automotive Glass Experts firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and designees as assigned. Password construction for the firewall will be consistent with the strong password creation practices outlined in the Automotive Glass Experts Password Policy.

The specific guidance and direction for information systems security is the responsibility of IT. Accordingly, IT will manage the configuration of the Automotive Glass Experts firewalls.

Automotive Glass Experts has contracted with a Third Party Vendor to manage the external firewalls. This vendor will be responsible for:

- Retention of the firewall rules
- Patch Management
- Review the firewall logs for:
- System errors
- Blocked web sites
- Attacks
- Sending alerts to the Automotive Glass Experts network administrators in the event of attacks or system errors
- Backing up the firewalls

# Vulnerability Assessment Policy

**Overview**
Vulnerability assessments, at Automotive Glass Experts, are necessary to manage the increasing number of threats, risks, and responsibilities. Vulnerabilities are not only internal and external, but there are also additional responsibilities and costs associated with ensuring compliance with laws and rules, while retaining business continuity and safety of Automotive Glass Experts and member data.

**Purpose**
The purpose of this policy is to establish standards for periodic vulnerability assessments. This policy reflects Automotive Glass Experts's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

This policy covers all computer and communication devices owned or operated by Automotive Glass Experts. This policy also covers any computer and communications device that is present on Automotive Glass Experts premises, but which may not be owned or operated by Automotive Glass Experts. Denial of Service testing or activities will not be performed.

**Policy Detail**
The operating system or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower the IT Department to perform periodic security risk assessments for determining the area of vulnerabilities and to initiate appropriate remediation. All employees are expected to cooperate fully with any risk assessment.

Vulnerabilities to the operating system or environment for information system resources must be identified and corrected to minimize the risks associated with them.

Audits may be conducted to:
- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents and to ensure conformance to Automotive Glass Experts's security policies
- Monitor user or system activity where appropriate

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment, the information system resource classification, and the data classification of the data associated with the information system resource.

Retesting will be performed to ensure the vulnerabilities have been corrected. An authenticated scan will be performed by either a Third-Party vendor or using an in-house product.

All data collected and/or used as part of the Vulnerability Assessment Process and related procedures will be formally documented and securely maintained.

IT leadership will make vulnerability scan reports and on-going correction or mitigation progress to senior management for consideration and reporting

# Website Privacy Policy

This Privacy Policy describes how your personal information is collected, used, and shared when you visit https://www.automotiveglassexperts.com/ (the "Site").

**Personal information**
While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you.

**Log Data**
Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data").

This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages, and other statistics.

In addition, we may use third-party services such as Google Analytics that collect, monitor, and analyze this information.

**Cookies**
"Cookies" are data files that are placed on your device or computer and often include an anonymous unique identifier. Cookies are used to improve our service to you. For more information about cookies, and how to disable cookies, visit https://www.allaboutcookies.org.

**Google Analytics**
Google Analytics is a web analysis service provided by Google Inc. ("Google"). Google utilizes the Data collected to track and examine the use of this Application, to prepare reports on its activities, and share them with other Google services.

Google may use the Data collected to contextualize and personalize the ads of its advertising network.

By filling in the contact form with their Data, the User authorizes this Site to use these details to reply to requests for information, quotes, or any other kind of request as indicated by the form's header.

By registering on the newsletter, the User's email address will be added to the contact list of those who may receive email messages containing information of commercial or promotional nature concerning this Site.

**How we use your personal information**
We use the Contact Information that we collect generally to fulfill any inquiry or quotes placed through the Site. Additionally, we use this information to:

Communicate with you, when in line with the preferences you have shared with us, provide you with information or advertising relating to our products or services.

We use the Device Information that we collect to help us screen for potential risk and fraud (in particular, your IP address), and more generally to improve and optimize our Site (for example, by generating analytics about how our customers browse and interact with the Site, and to assess the success of our marketing and advertising campaigns).

**Sharing your personal information**
We use Google Analytics to help us understand how our customers use the Site. You can read more about how Google uses your Personal Information here: https://www.google.com/intl/en/policies/privacy/. You can also opt out of Google Analytics here: https://tools.google.com/dlpage/gaoptout.

We may also share your Personal Information to comply with applicable laws and regulations, to respond to a subpoena, search warrant or other lawful requests for information we receive, or to otherwise protect our rights.

We may use your Personal Information to provide you with targeted advertisements or marketing communications we believe may be of interest to you. For more information about how targeted advertising works, you can visit the Network Advertising Initiative's ("NAI") educational page at https://www.networkadvertising.org/understanding-online-advertising/how-does-it-work

**Data retention**
When you place an inquiry through the Site, we will maintain your contact Information for our records unless and until you ask us to delete this information.

**Security**
The security of your Personal Information is important to us, but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

**Data breach**
In the event of a data breach, we will notify you within 72 hours of the breach and the steps taken to resolve the issue.

**Changes**
We may update this privacy policy from time to time to reflect, for example, changes to our practices or for other operational, legal, or regulatory reasons.

**Contact us**
For more information about our privacy practices, if you have questions, or if you would like to make a complaint, please contact us by e-mail at info@automotiveglassexperts.com

# Patch Management Policy

**Purpose**
Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing Automotive Glass Experts at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

Given the number of computer workstations and servers that comprise the Automotive Glass Experts network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches when they are made available. Effective security is a team effort involving the participation and support of every Automotive Glass Experts employee and the Board of Directors.

This policy is to assist in providing direction, establishing goals, enforcing governance, and to outline compliance.

**Audience**
This policy applies to all employees, contractors, consultants, temporaries, and the Board of Directors at Automotive Glass Experts. This policy applies to all equipment that is owned or leased by Automotive Glass Experts, such as, all electronic devices, servers, application software, computers, peripherals, routers, and switches. Adherence to this policy is mandatory.

**Policy Detail**
Many computer operating systems, such as Microsoft Windows, Linux, and others, include software application programs which may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the Automotive Glass Experts network, and all computers connected to it.

Almost all operating systems and many software applications have periodic security patches, released by the vendor, that need to be applied.

Patches, which are security related or critical in nature, should be installed as soon as possible.

- In the event that a critical or security related patch cannot be centrally deployed by IT, it must be installed in a timely manner using the best resources available.

- Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of policy.

**Responsibility**
The Director of IT is responsible for providing a secure network environment for Automotive Glass Experts. It is Automotive Glass Experts's policy to ensure all computer devices (including servers, desktops, printers, etc.) connected to Automotive Glass Experts's network, have the most recent operating system, security, and application patches installed.

Every user, both individually and within the organization, is responsible for ensuring prudent and responsible use of computing and network resources.

IT is responsible for ensuring all known and reasonable defenses are in place to reduce network vulnerabilities, while keeping the network operating.

IT Management and Administrators are responsible for monitoring security mailing lists, reviewing vendor notifications and Web sites, and researching specific public Web sites for the release of new patches. Monitoring will include, but not be limited to:

- Scheduled third party scanning of Automotive Glass Experts's network to identify known vulnerabilities
- Identifying and communicating identified vulnerabilities and/or security breaches to Automotive Glass Experts's Director of IT
- Monitoring Computer Emergency Readiness Team (CERT), notifications, and Web sites of all vendors that have hardware or software operating on Automotive Glass Experts's network

The IT Security and System Administrators are responsible for maintaining accuracy of patching procedures which detail the what, where, when, and how to eliminate confusion, establish routine, provide guidance, and enable practices to be auditable.

Documenting the implementation details provides the specifics of the patching process, which includes specific systems or groups of systems and the timeframes associated with patching.

Once alerted to a new patch, IT Administrators will download and review the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule.

# Data Protection Policy

**Overview**

- Where we refer to “process”, it means how we collect, use, store, make available, destroy, update, disclose, or otherwise deal with personal information. As a general rule we will only process this personal information if it is required to deliver or offer a service, provide a product, carry out a transaction or obligation in a contract.

- We may combine this personal information and use the combined personal information for any of the purposes stated in this Privacy Policy.

- If you use our other services, goods, products, and service channels you agree that we may process this personal information as explained under this Privacy Policy. Sometimes you may provide us with consent to process this personal information.

- Automotive Glass Experts is a global organisation and as such this Privacy Policy will apply to the processing of personal information by any member of Automotive Glass Experts globally. If Automotive Glass Experts processes personal information for another party under a contract or a mandate, the other party’s privacy policy will apply to the processing of such information.

- Automotive Glass Experts can change this Privacy Policy from time to time if the law or our business practices requires such change.

- This policy establishes a general standard for the appropriate protection of personal information (POPI) within the Automotive Glass Experts environment furthermore, it provides principles regarding the rights of individuals to privacy and to reasonable safeguards of their personal information.

**Scope**

All employees, contractors, consultants, temporary and other workers at Automotive Glass Experts, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Automotive Glass Experts, or to devices that connect to a Company network or reside at a Company site.

**Policy Statement**

**1.What is personal information?**

Personal information refers to any information that identifies you or specifically relates to you, or your employees stored or processed on The Product/s. Personal information includes, but is not limited to, the following information about you and / or your employees:

- Marital status
- National origin
- Age
- Language
- Birthplace
- Education
- Relevant financial history
- Identifying number (like an employee number, identity number or passport number)
- E-mail address; physical address (like residential address, work address or your physical location); telephone number

- Biometric information (like fingerprints, signature, or voice)
- Race; gender; sex; pregnancy status; ethnic origin; social origin; colour; sexual orientation
- Physical health; mental health; well-being; disability; religion; belief; conscience; culture
- Medical history; criminal history; employment history
- Personal views, preferences, and opinions
- Another's views or opinions about you.
- Full names and initials

Personal information includes special personal information, as explained below.

**2.When will we process your personal information?**

We will only process this personal information for lawful purposes relating to our business if the following applies:

- If you have consented thereto
- If a person legally authorised by you, the law, or a court, has consented thereto.
- If it is necessary to conclude or perform under a contract, we have with you
- If the law requires or permits it
- If it is required to protect or pursue your, our or a third party's legitimate interest.

**3.What is special personal information? Special personal information is personal information about the following:**

- Race (like where a company submits reports to the Department of Labour where the statistical information must be recorded)
- Ethnic origin
- Trade union membership
- Health (like where you apply for an insurance policy)
- Biometric information (like to verify your identity); and / or your criminal behaviour and alleged commission of an offense.

- **4.When will we process your special personal information?**
- We may process your special personal information in the following circumstances:
- If you have consented to the processing
- If the information is being used for any Human Resource or payroll related requirement
- If the processing is needed to create, use or protect a right or obligation in law.
- If the processing is for statistical or research purposes and all legal conditions are met
- If the special personal information was made public by you
- If the processing is required by law

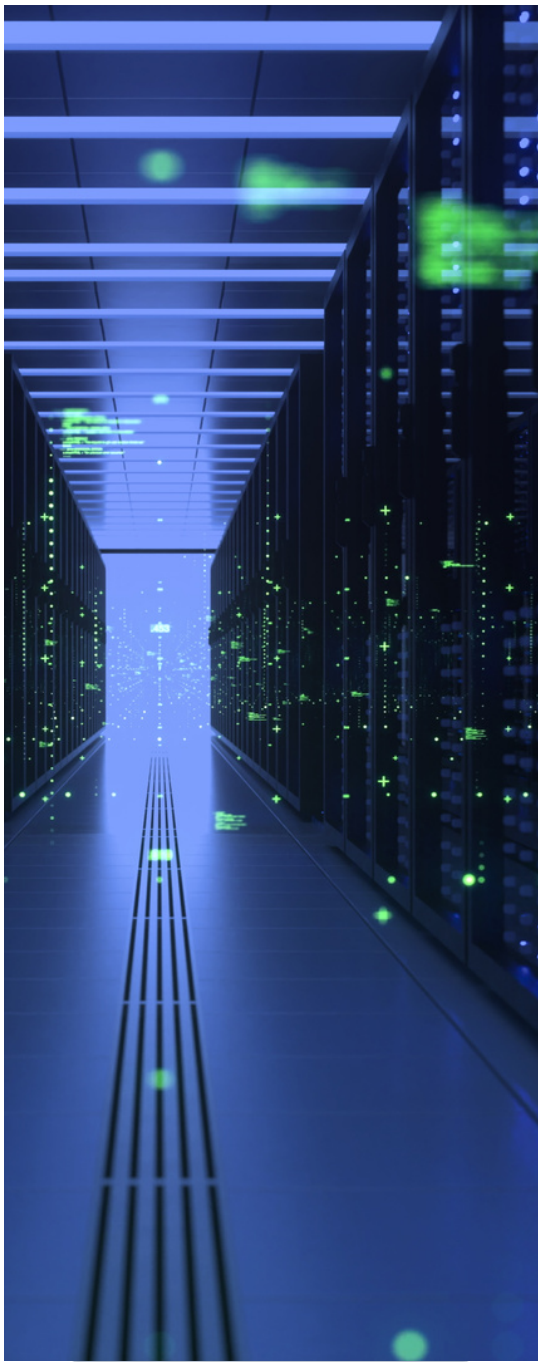
**5.When and from where we obtain personal information about you**

- We collect personal information from you directly.
- We may collect personal information from a public record or if you have deliberately made the information public.
- We collect personal information from 3rd parties that are directly integrated with our software platform.

We collect information about you based on your use of our products, services, or service channels.

- We collect information about you based on how you engage or interact with us such as via emails, letters, telephone calls and surveys.
- We collect personal information from completed forms i.e., contact and billing information. If the law requires us to do so, we will ask for your consent before collecting personal information.
- The third parties from whom we may collect your personal information include, but are not limited to, the following:

1. Our partners, your employer, employees directly, any of our other Bureau or channel partners and any connected companies, subsidiary companies, its associates, cessionaries, delegates, assigns, affiliates or successors in title and / or appointed third parties (like its authorised agents, partners, contractors, and suppliers) for any of the purposes identified in this Privacy Policy.
2. law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime.
3. regulatory authorities, industry ombudsman, governmental departments, local and international tax authorities.
4. trustees, Executors or Curators appointed by a court of law.
5. our service providers, agents and sub-contractors like couriers and other persons we use to offer and provide products and services to you.
6. courts of law or tribunals.



**6.Reasons we need to process your personal information.**

- We will process your personal information for the following reasons:
- to provide you with products, goods and services;
- to market our products, goods, and services to you.
- to respond to your enquiries and complaints.
- to comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions, and rules), voluntary and involuntary codes of conduct and industry agreements or to fulfill reporting requirements and information requests.
- to conduct market and behavioural research, including scoring and analysis to determine if you qualify for products and services or to determine your credit or insurance risk;
- to develop, test and improve products and services for you;
- for historical, statistical and research purposes, like market segmentation.
- to process payment instruments.
- to create, manufacture and print payment advice;
- to enable us to deliver goods, documents or notices to you;
- for security, identity verification and to check the accuracy of your personal information;
- to communicate with you and carry out your instructions and requests.
- for customer satisfaction surveys, promotional offerings.
- to enable you to take part in and make use of value-added products and services.
- to assess our lending and insurance risks; and / or
- for any other related purposes.

**7. How we use your personal information for marketing purposes**

- We will use your personal information to market our services, related products, and services to you.
- We may also market non-banking or non-financial products, goods, or services to you.
- We will do this in person, by post, telephone, or electronic channels such as SMS, email, and fax.
- If you are not our customer, or in any other instances where the law requires, we will only market to you by electronic communications with your consent.
- In all cases you can request us to stop sending marketing communications to you at any time

**8.When how and with whom we share your personal information**

In general, we will only share your personal information if any one or more of the following apply:

- If you have consented to this
- If it is necessary to conclude or perform under a contract, we have with you
- If the law requires it; and / or
- If it's necessary to protect or pursue your, our or a third party's legitimate interests.

Where required, each member of the company may share your personal information with the following persons. These persons have an obligation to keep your personal information secure and confidential.

- Other members of Automotive Glass Experts, its associates, cessionary, delegates, assigns, affiliates or successors in title and / or appointed third parties (like its authorised agents, partners, contractors, and suppliers) for any of the purposes identified in this Privacy Policy.
- Our employees as required by their employment conditions.
- Attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements.
- Payment processing services providers, merchants, banks, and other persons that assist with the processing of your payment instructions, like 3rd party EFT service providers.
- Law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime.
- Regulatory authorities, industry ombudsmen, governmental departments, local and international tax authorities, and other persons the law requires us to share your personal information with
- Our service providers, agents and sub-contractors like couriers and other persons we use to offer and provide products and services to you
- Persons to whom we have ceded our rights or delegated our obligations to under agreements, like where a business is sold
- Courts of law or tribunals that require the personal information to adjudicate referrals, actions or applications.
- Trustees, Executors or Curators appointed by a court of law
- Participating partners in our customer loyalty reward programmes, where you purchase goods, products and service or spend loyalty rewards; and / or our joint venture and other partners with whom we have concluded business agreements, for your benefit.

**9.Under what circumstances will we transfer your information to other countries?**
We will only transfer your personal information to third parties in another country in any one or more of the following circumstances:

Where your personal information will be adequately protected under the other country's laws or an agreement with the third-party recipient

Where the transfer is necessary to enter into or perform under a contract with you, or a contract with a third party that is in your interest.

Where you have consented to the transfer; and / or

Where it is not reasonably practical to obtain your consent, the transfer is in your interest.

This transfer will happen within the requirements and safeguards of the law. Where possible, the party processing your personal information in the other country will agree to apply the same level of protection as available by law in your country or if the other country's laws provide better protection the other country's laws would be agreed to and applied.

An example of us transferring your personal information to another country is where foreign payments take place if you purchase goods or services in a foreign country, or request that we facilitate salary payments to your employees in the countries.

**10.Your duties and rights about the personal information we have about you**

You must provide proof of identity when enforcing the rights below.

You must inform us when your personal information changes.

Please refer to our Promotion of Access to Information Act 2 of 2000 Manual (PAIA Manual) for further information on how you can give effect to the rights listed below.
You have the right to request access to the personal information we have about you by contacting us. This includes requesting:

- Confirmation that we hold your personal information.
- A copy or description of the record containing your personal information; and
- The identity or categories of third parties who have had access to your personal information.

You have the right to request us to correct or delete the personal information we have about you if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or we are no longer authorised to keep it. You must inform us of your request in writing. Please refer to our PAIA Manual for further information in this regard, like the process you should follow to give effect to this right. It may take up to 15 business days for the change to reflect on our systems. We may request documents from you to verify the change in personal information.

A specific agreement that you have entered with us may determine how you must change your personal information provided at the time when you entered into the specific agreement. Please adhere to these requirements. If the law requires us to keep the personal information, it will not be deleted upon your request. The deletion of certain personal information may lead to the termination of your relationship with us.

You may object on reasonable grounds to the processing of your personal information.
We will not be able to give effect to your objection if the processing of your personal information was and is permitted by law; you have provided consent to the processing and our processing done according to your consent or the processing is necessary to conclude or perform under a contract with you.

You must inform us of any objection in writing. Please refer to our PAIA Manual for further information in this regard, like the process you should follow to give effect to this right.

Where you have provided your consent for the processing of your personal information, you may withdraw your consent. If you withdraw your consent, we will explain the consequences to you. We may proceed to process your personal information even if you have withdrawn your consent if the law permits or requires it. It may take up to 15 business days for the change to reflect on our systems, during this time we may still process your personal information.

You have a right to file a complaint with us or any Regulator with jurisdiction about an alleged contravention of the protection of your personal information by us. We will address your complaint as far as possible.

**11.How we secure your personal information**
We will take appropriate and reasonable technical and organisational steps to protect your personal information according to industry best practices. Our security measures (including physical, technological, and procedural safeguards) will be appropriate and reasonable. This includes the following:

- Keeping our systems secure (like monitoring access and usage)
- Storing our records securely
- Controlling the access to our buildings, systems and/or records; and
- Safely destroying or deleting records
- Ensure compliance with international security standards

**12.How long do we keep your personal information?**
We will keep your personal information for as long as:

- The law requires us to keep it
- A contract between you and us requires us to keep it
- You have consented to us keeping it
- We are required to keep it to achieve the purposes listed in this Privacy Policy.
- We require it for statistical or research purposes.
- A code of conduct requires us to keep it; and / or
- We require it for our lawful business purposes.

Note: We may keep your personal information even if you no longer have a relationship with us, for the historical data that may be required by your employer or employee.

**13.Children's Privacy**
Our Service does not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If You are a parent or guardian and You are aware that Your child has provided Automotive Glass Experts with Personal Data, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 13 without verification of parental consent, we take steps to remove that information from Our servers.

If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, we may require Your parent's consent before We collect and use that information.

**14.Our cookie policy**

A cookie is a small piece of data sent from our websites or applications to your computer or device hard drive or Internet browser where it is saved. The cookie contains information to personalise your experience on our websites or applications and may improve your experience on the websites or applications. The cookie will also identify your device, like the computer or smart phone.

By using our websites or applications you agree that cookies may be forwarded from the relevant website or application to your computer or device. The cookie will enable us to know that you have visited the website or application before and will identify you. We may also use the cookie to prevent fraud and for analytics.

- References

| Document Name |
| --- |
| Information Classification Policy |
| PAIA Manual |
| |
| |
| |

- Outputs

The following records need to be kept and stored securely.

| Record | Responsible Person | Retention | Disposition |
| --- | --- | --- | --- |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

# Data Retention and Destruction Policy

**Purpose**
The purpose of this policy is to define the activities associated with the provision of data retention and destruction plans and programs that protect <Automotive Glass Experts> information systems, networks, data, databases and other information assets.

Additional policies governing data management activities will be addressed separately.

**Scope**
The scope of this data retention and destruction policy is all information technology systems, software, databases, applications and network resources needed by the Company to conduct its business.

**Statement of Compliance**
This policy is designed to be compliant with the U.S. Data Protection Act of 1998, Freedom of Information Act of 2000, Fair and Accurate Credit Transactions Act of 2003, Personal Information Protection and Electronic Documents Act in Canada, Gramm-Leach-Bliley Act, and Europe's General Data Protection Regulation.

**Data retention and destruction policy** compliance is managed by the IT department, with support from the digital department leadership and subject matter experts. To achieve compliance, data retention and destruction programs must include appropriate procedures, and identify staffing and technology resources to meet compliance requirements. Compliance verification (especially for data destruction) is performed monthly by the IT department, internal audit or other appropriate entity.

**Policy**
The Information Technology (IT) department is responsible for managing all data retention and destruction activities for the Company.

Other departments, such as Finance and Accounting, Operations and Human Resources, are also responsible for providing the IT department with their requirements for data retention and destruction. The IT department is responsible for developing, executing and periodically testing data retention and destruction procedures. The IT department also acknowledges it will comply with appropriate industry standards for data retention and destruction in its activities.

The company shall develop comprehensive data retention and destruction plans in accordance with good data management practices as defined by established standards.

Data retention and destruction activities shall be performed as part of the company's data management program, which administers and manages the overall technology data management program, which includes:

- Planning and design of data retention and destruction activities;
- Identification of data retention and destruction teams, defining their roles and responsibilities and ensuring they are properly trained and prepared to perform their duties;

- Planning, design and documentation of data retention and destruction plans;
- Scheduling of updates to data retention and destruction risk analyses;
- Planning and delivery of awareness and training activities for employees and data retention and destruction team members;
- Planning and execution of data retention and destruction plan exercises;
- Designing and implementing data retention and destruction maintenance activities to ensure that plans are up to date and ready for use;
- Preparing for management review and auditing of data retention and destruction plan(s); and
- Planning and implementation of continuous improvement activities for data retention and destruction activities and plans.
- Formal risk assessments (RAs) and business impact analyses (BIAs) shall include requirements for data retention and destruction activities; RAs and BIAs shall be updated at least annually to ensure they are in alignment with the business and its technology requirements.
- Data retention and destruction plans shall address electronic data stored on electronic media such as CDs, hard disk drives, solid state disk drives, magnetic tape and other appropriate media.
- Data retention and destruction plans shall address data stored on non-electronic media (e.g., paper files, microfiche).
- Data retention and destruction plans shall address electronic information systems (e.g., servers, routers, switches) and components (e.g., cabling and connectors, power supplies, storage racks) and other assets that are currently out of production or scheduled to be phased out of production environments.
- Data retention plans shall establish the storage requirements and associated metrics (e.g., length of storage, type of storage media) for electronic and non-electronic information as well as systems supporting the IT infrastructure.
- Data destruction plans shall establish the parameters for destruction of electronic data (e.g., overwriting, reformatting, degaussing, firmware-based erasure, physical data media destruction), non-electronic data (e.g., shredding of hard copy), and systems and components (e.g., third-party destruction services).

- Data retention and destruction plans shall be periodically reviewed and tested in a suitable environment to ensure that data, databases, media, systems and other relevant elements can be retained or destroyed and that <Automotive Glass Experts> management and employees understand how the plans are to be executed as well as their roles and responsibilities.

- All employees must be made aware of the data retention and destruction program and their own roles and responsibilities.

- Data retention and destruction plans and other documents are to be kept up to date and will reflect existing and changing circumstances.

- Data Retention and Destruction Specifications

Following are specific data retention and destruction technical requirements:

**General**

A script is run to identify records that need to be redacted.

The records retrieved have an anniversary date of 3 years and 1 month old.

Fields to be redacted are: First and Last names, ID numbers, email addresses and references to identity documents.

A script is run to redact and delete personal data. A count of redacted rows is returned for comparison to phase 1 output.

Members of the development team currently on the support rotation are responsible for running this operation.
A senior developer should immediately be notified in the event of some breakdown of this process.

**Data/System Retention Procedures**

- Data is stored on a MongoDB document DB hosted by Atlas in the AWS Cape Town Environment and enforced by tenant segregation.

- Identity document images are stored in S3 buckets and undergoes archival on the 3-year 1 month's anniversary.

Once redaction and deletion are completed a redaction document is updated by the support member and verified by a senior.

**Data/System Destruction Procedures**

On the First Tuesday of every month a developer runs stage 1 of a script to establish the quantum of the records to be redacted as well as retrieve the record ID`s to be redact based on the create date.

Phase 2 of the script is run against the ID`s to automatically update the pre identified personal information fields to "Redacted – {date}" and images of identity documents are deleted.

A senior developer confirms process completion by running a query to identify data that does not contain the text "Redacted" and is 3 years and 1 month old.

**Retention and Destruction Requests**
Data deletion requests are authorised by CIO and processed by a senior developer who compiles and signs a report of successful completion upon completing the request.

**Policy Leadership**
CIO, is designated as the corporate owner responsible for data/system retention and destruction activities for the Company.

Resolution of issues in the support of data/system retention and destruction activities should be coordinated with IT management and others as needed.

**Policy Responsibilities**

- Policy Approval – The CIO is responsible for approving this policy.
- Policy Implementation – The CTO is responsible for planning, organizing and implementing all activities that fulfill this policy.
- Policy Maintenance and Updating – The CTO is responsible for all activities associated with maintaining and updating this policy.
- Policy Monitoring and Review – The CTO is responsible for monitoring and reviewing this policy.
- Policy Improvement – The CTO is responsible for defining and implementing activities that will improve this policy.

**Penalties for Noncompliance**

In situations where it is determined that data retention and destruction activities do not comply with this policy, the IT department team assigned to this activity will prepare a report stating the reason(s) for noncompliance and present it to IT management for resolution. Failure to comply with this data retention and destruction policy within the allotted time for resolution may result in verbal reprimands, notes in personnel files, termination, and such other remedies as deemed appropriate.

# Incident Response & Recovery Plans

**Overview**
This policy is applicable to all departments and users of IT resources and assets.

- Cyber Incident Management

a. Entities must have an incident response plan, consistent standards, to effectively respond to security incidents.

b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Security Operations Center directly.

c. The Security Operations Center must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.
Associated Standard: Cyber Incident Response Standard

## Incident Recovery Plan

**Overview**
Since disasters happen so rarely, management often ignores the disaster recovery planning process.It is important to realize that having a contingency plan in the event of a disaster gives <Automotive Glass Experts> a competitive advantage.

This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions.Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

**Purpose**
This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by <Automotive Glass Experts> that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

**Scope**
This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date.This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

**Policy**
Automotive Glass Experts will create the following plans to respond to cybersecurity incidents:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

**Policy Compliance**
Compliance Measurement: The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions: Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Cybersecurity Incident Response Plan

**Purpose**

Automotive Glass Experts stores information related to Policyholders contact details, Insurance account information and policy holder vehicle information, as well as manages and maintains technical infrastructure required and claims management system to house and maintain this information.

Additionally, Automotive Glass Experts has contracts with vendors of digital services and products to manage and maintain this data and infrastructure.

This Cyber Security Incident Response Plan outlines the procedures Automotive Glass Experts uses to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained or serviced by their contracted suppliers. More specifically, this plan defines the roles and responsibilities of various Automotive Glass Experts staff with respect to the identification, isolation and repair of data security breaches, outlines the timing, direction and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response.

Automotive Glass Experts makes use of appropriate physical security and environmental controls for technical infrastructure, and deploys digital security measures such as firewalls, malware detection, ransomware and other industry standard prevention systems.

**Definitions**

- **Cyber Security Incident**

A Cyber Security Incident is any event that threatens the confidentiality, integrity or availability of the information resources we as Automotive Glass Experts and our partners support or utilize internally, especially sensitive information whose theft or loss may be harmful to individual policy holders, our partners or our organization.

- **Incident Response Team (IRT).**

The IRT is made up of individuals across different fields in the organization whose charge is to navigate the organization through a Cyber Security Incident from the initial investigation to mitigation, to post incident review. Members include an Incident Response Manager, technical hardware and networking experts, front-end software experts, communications experts and legal experts.

- **Incident Response Manager (IRM).**

The IRM oversees all aspects of the Cyber Security Incident, especially the IRT. The key focuses of the IRM will be to ensure proper implementation of the procedures outlined in the Cyber Security Incident Response Plan, to keep appropriate Incident Logs throughout the incident, and to act as the key liaison between IRT experts and the organization's management team. At the conclusion of a Cyber Security Incident, the IRM will conduct a review of the incident and produce both an Incident Summary Report and a Process Improvement Plan.

- **Cyber Security Incident Log.**

The Cyber Security Incident Log will capture critical information about a Cyber Security Incident and the organizations response to that incident and should be maintained while the incident is in progress.

- **Incident Summary Report (ISR).**

The ISR is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide a detailed summary of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the procedures of the Cyber Security Incident Response Plan, including how the IRT followed the procedures and whether updates are required. The template for the ISR may be seen in Annexure A.

- **Process Improvement Plan (PIP).**

The PIP is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide recommendations for avoiding or minimizing the impact of future Cyber Security Incidents based upon the "lessons learned" from the recently-completed incident. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Annexure B.

**Incident Response Team**
Name: Nicholas Karlsen
Email: nicholask@apollostudios.co.za
Cell: +27 83 603 3863

**Technical contacts**
Name: Anil Dhawade
Email: anil@apollost5udios.co.za
Cell: +27 84 782 4772

**Hosting Contacts**
Name: Google
URL:
https://firebase.google.com/support/troubleshooter/contact

**Legal Counsel**
Name: TBA
Email:
Cell:

**Communications specialist**
Name: Carina Feliciano
Email:
marketing@automotiveglassexperts.com
Cell: +351 993 017 092

## Incident Management Principles Confidentiality

**Investigation**
During a Cyber Security Incident investigation, the IRM or members of the IRT will be gathering information from multiple computer systems and/or conducting interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Cyber Security Incident will be strictly confidential throughout the investigative process. At the conclusion of the investigative process, the IRM will brief the Automotive Glass Experts executive on the relevant details of the incident and the investigation. During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself.

**Affected Stakeholders**
In the event the incident involves the unauthorized access or disclosure of policy holder information, Automotive Glass Experts will communicate information relevant to the incident as well as any additional requested information. Automotive Glass Experts does reserve the right to withhold certain information at the discretion of the IRM if that information may jeopardize current or future investigations, or pose a security risk to Automotive Glass Experts or other entities.
In the event the incident involves information of an non-Automotive Glass Experts stakeholder, such as an Insurer, Policy holder or vendor partner, Automotive Glass Experts will take appropriate steps to notify those entities as efficiently as possible. In the event the incident is limited to Automotive Glass Experts systems not containing sensitive or confidential information, it will be the discretion of the Automotive Glass Experts Executive and the IRM whether or not to share information related to the incident with outside stakeholders.

## Cyber Security Incident Phases Identify

**Overview**
All Automotive Glass Experts staff have a responsibility to remain vigilant and protect the data stored within the systems we support. Any event that threatens the confidentiality, integrity or availability of the information resources we support or utilise internally should immediately be reported to a supervisor or the IRM if a supervisor is unavailable. Supervisors should immediately bring the incident to the attention of the IRM. Automotive Glass Experts partners are also encouraged to notify the Technical support team by email development@AutomotiveGlassExperts.co.za, alerting them to the suspected data breach.

**Incident Types**

Types of cyber incidents that may threaten the organization are:

- Unauthorized attempts to gain access to a computer, system or the data within
- Service disruption, including Denial of Service (DoS) attack
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, corruption or unauthorized distribution

**Incident Symptoms**

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content or activity
- Locally hosted websites won't open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behaviour or activity by Automotive Glass Experts staff, partners or other related actors.

## Assess

**Overview**

Once anomalous activity has been reported, it is incumbent upon the IRM to determine the level of intervention required. Other members of the IRT may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion, the IRM will alert the entire IRT immediately so that the situation may be dealt with as expeditiously as possible.

**Considerations**

- What are the symptoms?
- What may be the cause?
- What systems have been / are being / will be impacted?
- How wide spread is it?
- Which stakeholders are affected?

**Documentation**

Regardless of whether it is determined there is a security threat, the IRM will accurately document the scenario in a Cyber Security Incident Log. All Cyber Security Incident Logs will be stored in a single location so that incident information may be reviewed in the future. This report should contain information such as:

- Who reported the incident
- Characteristics of the activity
- Date and time the potential incident was detected

- Nature of the incident (Unauthorized access, DDoS, Malicious Code, No Incident Occurred, etc.)
- Potential scope of impact
- Whether the IRT was required to perform incident remediation.

## Respond

**Briefing of Administration**

Upon determining that a significant incident or breach has occurred, the Automotive Glass Experts Executive should be notified immediately. As additional information is uncovered throughout the investigation, the executive should be briefed by the IRM so appropriate decisions, such as allocating additional staff, hiring outside consultants and involving law enforcement can be made. Additionally, based on the incident, it will be incumbent on Administration to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so. The Executive should take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws and the communication requirements of all parties involved.

A list of FNB recipients to be notified are found in Annexure D.

**Initial Response**

This first steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve measures up to and including immediately disconnecting workstations, servers or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas, to define the entire scope of the incident.

Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems have been restored.

**Remediation and Recovery**

Once the cause has been determined and appropriately isolated, the IRT will need to remove the vulnerabilities leading to the incident. This may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the IRM
- Closely monitor the systems once reconnected to the network

## Report

### Overview

Once the threat has been mitigated and normal operation is restored, the IRM will compile all available information to produce an accurate and in-depth summary of the incident in an Incident Summary Report (ISR). A copy of the ISR is located in Annexure A. Throughout the incident, the IRT will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report. Interviews will also be conducted with appropriate members of the IRT to obtain any additional information that may be available to augment the logs and records kept throughout the process.

### Report Contents

The Incident Summary Report (ISR) will include all pertinent information to the incident, but at minimum:

- Dates and times of milestones throughout the process (e.g. incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of memos, emails, etc. where possible)

### Timeframe

The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the IRT should be conducted immediately to ensure the greatest possible accuracy of information.

## Review

### Post-Incident Review Meeting

After the conclusion of the incident, the IRM and possibly select members from the IRT will meet with management to discuss the event in detail, review response procedures and construct a Process Improvement Plan (PIP) to prevent a reoccurrence of that or similar incidents. The compiled Incident Report constructed by the IRM will serve as a guide for this meeting.

In the meeting, a full debrief of the incident will be presented and findings discussed. The IRM will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

As a whole, the group will review the information presented and will determine any weakness in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

**Process Improvement Plan**
The IRM will draft a Process Improvement Plan (PIP) based on the results of this meeting. The plan should discuss any applicable items necessary to, prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are met in a timely fashion and functioning appropriately. Areas of focus may include, but are not limited to:

- New hardware or software required
- Patch or upgrade plans
- Training plans (Technical, end users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan
- Regional communications recommendations

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required to clients or to the public must be drafted separately and include only information required to prevent future incidents.

# Annexure A

**Incident Summary Report**

| Type of Incident | |
|---|---|
| Date Incident Originated | |
| Date Incident Was Detected | |
| By Whom Was Incident Detected | |
| How Was Incident Detected | |
| Scope of Incident (Districts/ Systems Affected) | |
| Date Incident Corrected | |
| Corrective Action Types (Training, Technical, etc) | |

Summary of Incident Symptoms:
Summary of Incident Type and Scope:
Summary of Corrective Actions:
Summary of Mitigation Processes and Internal Communication:

**Communications Log (Attach drafts for written communications, synopsis for verbal communication)**

| Communication Date | Communication Type | Recipients | Purpose |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Annexure B

**Process Improvement Plan**

Areas of Success Summary:

Areas in Need of Improvement Summary:

Recommended Improvements to Avoid Future Incidents:

Recommended Improvements to the Cyber Security Incident Response Plan:

| Improvement | Timeframe | Cost |
|---|---|---|
| | | |
| | | |
| | | |

# Annexure C

**Incident Log**

Incident Title :

Incident Opened Date:

Incident Description:

| Action / Event | Date/ Time | Performed By | Details |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Terms

**Firewall:** Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.
Firewall configuration: The system setting affecting the operation of a firewall appliance.

**Firewall ruleset:** A set of policy statements or instructions used by a firewall to filter network traffic.

**Host firewall:** A firewall application that addresses a separate and distinct host, such as a personal computer.

**Internet Protocol (IP):** Primary network protocol used on the Internet.

**Network firewall:** A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).

**Network topology:** The layout of connections (links, nodes, etc.) of a computer network.
Simple Mail Transfer Protocol (SMTP): An Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

**Virtual private network (VPN):** A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with private, secure access to their organization's network.
Dictionary attacks: An attempt to gain illicit access to a computer system by using a very large set of words to generate potential passwords.

**Local Administrator Password Solution (LAPS):** For environments in which users are required to log on to computers without domain credentials, password management can become a complex issue. Such environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack. The Local Administrator Password Solution (LAPS) provides a solution to this issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain. Domain administrators using the solution can determine which users, such as helpdesk administrators, are authorized to read passwords.

**SuperUser / Administrator:** A user of a computer system with special privileges needed to administer and maintain the system

**Domain:** In computing and telecommunication in general, a domain is a sphere of knowledge identified by a name. Typically, the knowledge is a collection of facts about some program entities or a number of network points or addresses.

**Account:** Any combination of a User ID (sometime referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.

**System Administrator:** The person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

**Cloud computing:** Is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.

**Public cloud:** Is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

**Private Cloud:** Is based on the standard cloud computing model but uses a proprietary architecture at an organization's in-house facilities or uses an infrastructure dedicated to a single organization.

**Financial information:** Is any data for Automotive Glass Experts, its employees, members, or other third parties.

**Intellectual property:** Is any data that is owned by Automotive Glass Experts or provided by a third party that would not be distributed to the public.

**Other non-public data or information:** Are assets deemed the property of Automotive Glass Experts.

**Other public data or information:** Are assets deemed the property of Automotive Glass Experts.

**Personally Identifiable Information (PII):** Is any data that contains personally identifiable information concerning any members, employees, or other third parties.

# Agreements

## Operator's Agreement

| | | |
|---|---|---|
| AGE® | Authorised by: | |
| | Date Authorised: | |
| | Document Number: | **006/2021/009** |

**Operator's Agreement**
entered into by and between:

**Name:**
**Registration number:**
(Hereinafter to be referred to as: the **"Responsible Party"**),

**AND**

**Name:**
**Registration number/Identity number:**
(Hereinafter to be referred to as: the **"Operator"**),

**Hereby Agree as Follows:**

**1. Definitions And Interpretations:**

1.1. In this agreement:

1.1.1. Clause headings are for convenience and shall not be used in its interpretation and unless the context clearly indicates a contrary intention.

1.1.2. An expression which denotes any gender includes the other gender; a natural person includes an artificial or juristic person and vice versa; the singular includes the plural and vice versa.

1.1.3.The following words shall bear the meanings assigned to them below:

1.1.3.1. "Agreement" means this Operator Agreements and any schedules attached hereto.

1.1.3.2. "Data subject" means the person to whom personal information relates.

1.1.3.3. "Information officer" of, or in relation to, a –

1.1.3.4. Public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of this Act; or

1.1.3.5. Private body means the head of a private body as contemplated in Section 1, of PAIA.

1.1.4."Operator" means a person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party.

1.1.5."Personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

1.1.5.1. Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.

1.1.5.2. Information relating to the education or the medical, financial, criminal or employment history of the person.

1.1.5.3. Any identifying number, symbol, e-mail address, telephone number, location information, online identifier, or other particular assignment to the person.

1.1.5.4. The biometric information of the person.

1.1.5.5. The personal opinions, views, or preferences of the person.

1.1.5.6. Correspondence sent by the person that would reveal the contents of the original correspondence.

1.1.5.7. The views or opinions of another individual about the person; and

1.1.5.8. The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

1.1.6."Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

1.1.6.1. The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.

1.1.6.2. Dissemination by means of transmission, distribution or making available in any other form; or

1.1.6.3. Merging, linking, as well as restriction, degradation, erasure, or destruction of information.

1.1.7."PAIA" means the Promotion of Access to Information Act No. 2 of 2000.

1.1.8."POPI": means the Protection of Personal information Act No. 4 of 2013.

1.1.9."Responsible Party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

**2. Application:**

2.1. This Agreement shall apply to all processing of personal information that may be subject to POPI in the scope of all agreements, currently entered into between the parties.

2.2. Insofar as the Operator will be processing personal information subject to POPI on behalf of the Responsible Party during the performance of the Operator's obligations in terms of the agreements referred to in clause 2.1.

2.3. In the event of a conflict between any provisions of the agreements as referred to in clause 2.4. and the provisions of this agreement, the provisions of this Agreement shall prevail.

2.5. An overview of the categories of personal information, the categories of Data Subjects, and the nature and purposes for which the personal information are being processed is provided in Schedule 2.

**3. Duration And Termination:**

3.1. This Agreement shall come into effect on the date of the last signature being appended unto this Agreement.

3.2. This Agreement may be terminated by either party upon 30 (thirty) days written notice.

3.3. Termination or expiration of this Agreement shall not discharge the Operator from its confidentiality obligations in terms of this agreement.

3.4. The Operator shall process personal information until the date of termination of this Agreement, or until such data is returned or destroyed on instruction of the Responsible Party.

3.5. It is noted between the parties that should this agreement be terminated in terms of clause
3.3. of this agreement, the Operator may not be able to fulfil all its obligations in terms of the agreements as detailed in clause 2.1 due to requirements in POPI not being met.

**4. The Responsible Party and The Operator:**

4.1. The Operator will not process any personal information on behalf of the Responsible Party unless explicitly instructed to do so by the Responsible Party.

4.2. The Operator hereby undertakes that it will not process any personal information on behalf of the Responsible Party without the Responsible Party's knowledge and authorization.

4.3. Subject to the provisions of the agreements referred to in clause 2.1, to the extent that the Operator's personal information processing activities are not adequately defined in the agreements referred to in clause 2.1, the Responsible Party will determine: -

4.3.1.the parameters.

4.3.2.Purposes; and

4.3.3.the manner

by which the personal information may be processed by the Operator.

4.4. The Operator will process the personal information only on Responsible Party's written instructions and within the parameters as set forth in the Responsible Party's written instructions.

4.5. The Operator will only process the personal information to the extent that this is required for the provision of the services.

4.6. The Operator will inform the Responsible Party if the Operator is under a legal obligation to process the personal information in a manner which is beyond the scope of the Responsible Party's written instructions.

4.7. The Responsible Party warrants that it has the necessary consent and/or justification exists in terms of POPI for the processing to be performed in relation to the services.

4.8. Should the consent be revoked by a Data Subject and/or a justification for the processing activity no longer exist, the Responsible Party is responsible for communicating the fact of such revocation and/or termination to the Operator.

4.9. Should the Responsible Party communicate the revocation of consent and/or the termination of a justification in terms of POPI, the Operator will immediately cease to process the personal information that is associated with the said revocation and/or termination.

**5. Confidentiality:**

5.1. The Operator hereby undertakes to keep all personal information provided to it by the Responsible Party as confidential and shall not disclose the personal information without the Responsible Party's written consent.

5.2. The Operator shall inform all its employees, agents and/ or approved sub-Operators engaged in processing the personal information of the confidential nature of the personal information. The Operator will ensure that its employees, agents and/ or approved sub-Operators have entered into the necessary contractual agreements in order to ensure that all personal information is kept confidential, and the Operator will take action against its employees, agents and/ or approved sub-Operators in the event that they breach the aforementioned contractual agreements.

**6. Security:**

6.1. The Operator shall secure the integrity and confidentiality of the personal information in its possession or under its control by taking appropriate, reasonable technical and organizational measures to prevent:

6.1.1.The loss of damage to or unauthorized destruction of personal information; and

6.1.2.Unlawful access to or processing of the personal information.

6.2. the Operator must take reasonable measures to—

6.2.1. identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

6.2.2. establish and maintain appropriate safeguards against the risks identified;

6.2.3. regularly verify that the safeguards are effectively implemented; and

6.2.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

6.3. The Operator must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

6.4. The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

**7. Transborder Information Flow**

7.1. The Operator shall notify the Responsible Party of any planned transfers of personal information to a third party who is in a foreign country, prior to the transfer and the Operator will inform the Responsible party of the level of protection the personal information will have in the third party's possession.

7.2. The Operator will not make any transborder transfer without the Responsible Party's written authorisation.

**8. Notification Of Security Compromises:**

8.1.Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Responsible Party.

8.2.The notification referred to in clause 8.1 must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Operator's information system.

8.3.The notification referred to in clause 8.1 must provide sufficient information to allow the Responsible Party and/or data subject to take protective measures against the potential consequences of the compromise, including—

8.4.a description of the possible consequences of the security compromise.

8.5.a description of the measures that the Operator intends to take or has taken to address the security compromise.

8.6.a recommendation with regard to the measures to be taken by the Responsible Party and/or data subject to mitigate the possible adverse effects of the security compromise; and

8.7.if known to the Operator, the identity of the unauthorised person who may have accessed or acquired the personal information.

**9. Sub-Operators**

9.1. The Operator shall obtain the Responsible Party's written authorisation before it subcontract any of the processing operations as required in the agreements in clause 2.1.

9.2. The Operator shall remain fully will all obligations in terms of this Agreement and the agreements as set out in clause 2.1.

9.3. The Operator shall ensure that an Operator Agreement, comparable to this agreement, is signed between the Operator and any approved sub-operator.

**10. Returning Or Destruction of Personal Information:**

10.1. Upon termination of this Agreement, the Responsible Party's written instruction or the fulfilment of the obligation in the agreements as detailed in clause 2.1, the Operator shall, at the discretion of the Responsible Party, either delete, destroy, or return all personal information to the Responsible Party and destroy or return any existing copies of the personal information (should any exist).

10.2. The Operator shall notify all third parties supporting its own processing of the personal information of the termination of this Agreement and shall ensure that all such third parties shall either destroy the personal information or return the personal information to the Responsible Party, at the discretion of the Responsible Party.

**11. Miscellaneous:**

11.1. The Laws of the Republic of South Africa shall at all times govern this agreement and the contractual relationship between the parties.

11.2. The Operator shall not assign, cede, delegate, transfer or otherwise dispose of any right or obligation under this agreement to any other person, unless done in terms of this Agreement.

11.3. No provision of this agreement (including, without limitation, the provisions of this clause) may be amended, substituted, or otherwise varied, and no provision may be added to or incorporated in this agreement, except by a written agreements signed by the duly authorized representatives of each party.

11.4. Any indulgence by the Responsible Party in exercising, or any failure by the Responsible Party to exercise, any right under this agreement shall not be construed as a waiver of that right and shall not affect the ability of the Responsible Party subsequently to exercise that right or to pursue any remedy, nor shall any indulgence constitute a waiver of any right (whether against the Operator or any other person).

11.5. The waiver of any right under this agreement shall be binding on the waiving party only to the extent that the waiver has been reduced to writing and signed by the duly authorized representatives of the waiving party.

11.6. This agreement supersedes all prior agreements representations, communications, negotiations, and understandings between the parties concerning the subject matter of the agreement.

11.7. Whenever possible, each provision of the agreement shall be interpreted in a manner which makes it effect and valid under the applicable law but if any provision of the agreement is held to be illegal, invalid, or unenforceable under the applicable law, the offending clause shall be severed from the agreement and the offending clause shall not affect the other provisions of this agreement which will remain in full force and affect.

11.8. The parties choose the following addresses as their respective domicillia citandi et executandi at which all documents and notices, including those of a legal nature, can be delivered and/or served. The parties must notify the other party of any change in domicillia citandi et executandi.

| The Responsible Party | |
|---|---|
| Contact Number | |
| Address | |
| Email | |

| The Operator | |
|---|---|
| Contact Number | |
| Mobile Number | |
| Address | |
| Email | |
| VAT number | |

1. The parties agree to perform or procure the performance, of all further things, and execute and deliver (or procure the execution and delivery) of all further documents, as may be required by law or as may be desirable or necessary to implement or give effect to this agreement and the transactions contemplated herein.
2. The headings in this agreement will not be used in the interpretation of this agreement and are merely for ease of reference.

Thus, Done and Signed at on This Day Of 20__.

Name:
ID:
Contact:
Email:

Signature:
(The responsable Party)

Name:
ID:
Contact:
Email:

Signature:
(The responsable Party witness)

Who warrants his/her authority hereto.

Thus, Done and Signed at on This Day Of 20__.

Name:
ID:
Contact:
Email:

Signature:
(The Operator)

Name:
ID:
Contact:
Email:

Signature:
(The Operator witness)

Who warrants his/her authority hereto.

## Schedule 1

**Contact Information of the information officer of the responsible party**

Name and Surname:
Contact number:
Email address:

**Contact Information of the information officer of the operator**

Name and Surname:
Contact number:
Email address:

## Schedule 2

**Types of Personal information that will be processed in the scope of the agreements referred to in clause 2.1.**

Categories of Data Subjects:

Nature and purpose of the information processing:

# Together, **Creating Change**

AGE®