

Information Security Policy

General

Showell's Information Security Policy is based on ISO/IEC 27001:2022 Information Security Management ISO/IEC Standards. The Information Security Policy serves as the foundation for all Showell's Global Information Security and Privacy activities, and as a guide for implementing practices to minimize risk to the Showell's operations. This Policy has been created to define the methods with which Showell protects and secures data that Showell collects, stores, and processes.

Showell is committed to upholding effective security controls, encompassing aspects such as software development, change management, capacity planning, malware defense, data backup, logging, monitoring, and vulnerability management. In addition, appropriate measures will be maintained for communication security, which includes ensuring network security, segregation, management of network services, secure information transfer, and secure messaging. Furthermore, Showell will ensure the security of its people and facilities.

Purpose and Scope

This document outlines Showell's approach to information security, applicable globally to all systems, networks, and data resources managed by the company. It serves as a high-level guide for incorporating information security into Showell's corporate vision and daily operations. Detailed procedures and specific security aspects are covered in related Showell policy documents.

Importance of Information Security at Showell:

- Ensures reliable service delivery.
- Complies with international laws and regulations.
- Protects client data and privacy.
- Meets customer and regulatory security expectations.
- Manages and mitigates risks to business operations.

Showell's management commits to a high standard of information security and will allocate the necessary resources to uphold this policy across all company activities. This policy applies to all Showell employees, consultants, contractors, and affiliates. Non-compliance may lead to disciplinary actions, including possible termination of employment or affiliation.

Roles & Responsibilities

Responsibility to follow this policy applies to all Showell employees. The CISO and the Security Steering Committee are responsible for developing, maintaining, and implementing the Information Security Policy while the IT & Security Team is responsible for overseeing daily operations and activities together with HR and Department Managers (Team Leaders).

The roles and responsibilities at Showell are set out in the Roles and Responsibility Policy.

Security Forum/Steering Committee

The Security Steering Committee (SSC) acts as an advisory and review board to the CISO. The committee will provide a broader view of the company's requirements and goals, by including representatives from various departments which have interfaces to information security. The duties of SSC are:

- Review security activities performed in the past quarter and planned activities for the next quarter.
- Review and approve changes to this policy (annually).
- Review and approve the information security work plan (annually).
- Review information security incidents, their management, and lessons learned from them.

Policy Framework Details

Showell's current business strategy and framework for information security are the guidelines used for identifying, assessing, evaluating, and controlling information-related risks, through establishing and maintaining the Global Information Security Policy (this document).

Showell management has decided that information security is to be ensured through the application of the policy for information security, and a set of underlying and supplemental documents (such as security procedures and guidelines). To secure operations at Showell, Showell shall ensure the availability of continuity plans, backup procedures, defense against damaging code and malicious activities, system and information access controls, incident management, and reporting, even after serious incidents.

The term Information Security is related to the following basic concepts:

- **Confidentiality:** The concept that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** The concept of safeguarding the accuracy and completeness of assets.
- **Availability:** The concept of information and assets being accessible and usable upon demand by an authorized entity.

Continuous Information Security Enhancement and Compliance

Showell recognizes the need to keep the information security environment current on an ongoing basis. To achieve this goal, it has implemented the following:

- Periodic review of the security policies.
- Periodic updates (including security patches) of operational software, hardware, and other systems.
- Periodic penetration test and Vulnerability Assessment.
- Ongoing monitoring of key systems
- Tracking of security-related tasks to closure.
- Building education and awareness amongst personnel and partners
- Improve security to all information transfer, storage, and processing.

Important records are protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Organizational records shall be categorized into record types, e.g. database records, transaction logs, audit logs, and operational procedures each with details of the retention period and type of storage media (e.g. paper, optical media, magnetic media, etc.).

Showell identifies compliance requirements, including contractual, regulatory, and legal requirements, and shall integrate them into the company information security management processes as required.

Security Goals

At Showell, our commitment to information security is driven by the need to protect our physical and electronic assets while fulfilling regulatory, operational, and contractual obligations. Our approach encompasses several key areas:

- **Policy and Incident Management:** We will define and implement policies for managing cyber incidents and establish a robust cybersecurity program.
- **Guidance and Awareness:** We provide support and documentation to ensure awareness and understanding of information security among all relevant parties.
- **Integration into Business Operations:** Cybersecurity is integrated into both the strategic and operational aspects of our business.
- **Development of Security Programs:** We focus on developing and implementing comprehensive information security and privacy programs.
- **Cyber Threat Research:** We actively engage in ongoing research to stay ahead of emerging risks and trends in cybersecurity, ensuring our information assets and computing systems are resilient against the latest threats.
- **Continuous Review:** Regularly reviewing and updating our cybersecurity and privacy programs to keep pace with evolving threats.

Key Information Security Objectives:

- **Regulatory Compliance:** Adhere to relevant laws, regulations, and guidelines.
- **Confidentiality, Integrity, and Availability:** Meet these core requirements for all stakeholders.
- **Asset Protection:** Establish controls to protect against theft, abuse, and loss.
- **Responsibility and Ownership:** Encourage a security-conscious culture among staff.
- **Resilience:** Maintain service continuity even during major security incidents.

- Data Privacy: Protect personal and sensitive information.
- Network Reliability: Ensure the reliability and availability of network infrastructure and services.
- ISO 27001:2022 Standards: Comply with these information security and privacy standards.
- Vendor Compliance: Ensure external service providers meet our security and privacy standards.
- Remote Access Security: Maintain flexible yet secure access to information systems remotely.

Verification and Measurement

At Showell, we ensure the effectiveness of our information security through a comprehensive verification and measurement process. This involves a regular review of how our security measures and plan are implemented compared to the original design, allowing us to identify and rectify any discrepancies. Additionally, we conduct an annual analysis of information security incidents, assessing both the number and severity of incidents in comparison to the previous year. This helps us understand trends and make necessary adjustments. Complementing our internal reviews, we also engage in a yearly external audit to independently verify our security status against security targets. These combined efforts enable Showell to continuously refine and strengthen our security posture.

Laws and Regulations

Showell is committed to complying with all laws and regulations related to personal data processing and data privacy in the regions where we operate. This includes, but is not limited to, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Payment Card Industry Data Security Standard (PCI DSS), Israel's Privacy Protection Law (5741-1981), Switzerland's Data Protection Ordinance (DPO), and other relevant national laws and regulations.

These regulations significantly impact data management practices, such as backup requirements for accounting systems and data retention for employee information. The Legal Department is tasked with identifying new relevant laws and monitoring changes to existing legislation. Additionally, the CISO oversees the ongoing evolution of technology used by Showell and monitors information security risks.

Intellectual Property Rights

Our Information Security Management Policy strictly upholds Intellectual Property Rights (IPR). We ensure compliance with all relevant IPR laws and guidelines, firmly prohibiting unauthorized use or distribution of intellectual property in all our operations. This commitment reflects our dedication to ethical and legal integrity in our business practices.

Facilities and Premises Security

Showell prioritizes robust physical security measures as part of its information security framework. Key aspects include:

- Restricted access to facilities with a visitor management system. Employees use personal access keys, and visitors are always escorted.
- Sensitive documents and assets are stored in secure, locked areas.
- Strict sign-in/out procedures for visitors and deliveries.
- Clear Desk and Clear Screen policies ensure the security of information and devices.
- Fire alarms and safety systems, with regular employee safety briefings.
- 24/7 security surveillance, security guards, and cameras in place at company premises

For more comprehensive guidelines and detailed protocols, refer to the Physical Security Policy.

Cloud Security

Showell's Cloud, operated by Amazon Web Services (AWS), integrates robust security measures and AWS's top-notch perimeter defense to ensure the highest level of protection for our cloud-based operations.

- **AWS Cloud Infrastructure:** Our architecture in AWS includes detailed maps and data flow diagrams, regularly updated and reviewed.
- **Network Segmentation and Monitoring:** We utilize segregated environments within AWS, including development/staging and production, each with tailored security controls. Continuous cloud-based monitoring and threat detection systems are in place, ensuring real-time security oversight.

- **Perimeter Defense:** AWS's perimeter security is renowned for its strength, including advanced firewalls, intrusion detection, and a layered security approach. These measures effectively safeguard against external threats.
- **Authentication and Network Controls:** All connections and systems in our AWS network are strictly authenticated and authorized. Firewall and router configurations are rigorously managed and reviewed, adhering to the principle of least privilege.
- **DDoS Protection, Traffic Filtering, and Malware Defense:** We utilize AWS's DDoS mitigation services, enforce traffic filtering rules, and have robust malware and virus protection measures in place for enhanced security.
- **Compliance and Security Audits:** AWS complies with major certifications and standards, including ISO 27001, SOC 1, SOC 2, and PCI DSS, ensuring adherence to global security best practices.

Our Chief Information Security Officer (CISO) oversees these cloud security measures, with AWS managing the security and availability of the infrastructure. This integrated approach to Cloud Security ensures that Showell's cloud services are secure, resilient, and compliant with industry standards.

For a comprehensive view of our Cloud Security policies and practices, please refer to the System and Network Management Policy.

Asset Management

Showell maintains an up-to-date inventory of all its assets (data, software, hardware, etc.), regardless of their physical and geographical location. Each asset is assigned an owner, who is designated by the Chief Information Security Officer (CISO) in collaboration with the Management team and Department Managers. Only internal Showell employees can be appointed as information asset owners. All assets will be classified, to ensure that all information receives the appropriate level of protection, including encryption and hardening when required.

For additional information regarding the Company data classification process, refer to the Data Classification Policy. For additional information regarding the Company inventory of

assets, refer to Asset Management Policy.

Asset Changes

The responsibilities of an Asset Owner include:

- Determining the sensitivity level of the asset.
- Assessing the criticality level of the asset.
- Evaluating the risk level associated with the asset.
- Identifying the type of data stored in the asset.
- Raising awareness about the security features and requirements of the asset.

Changes in asset ownership require approval from the CISO.

Data Classification and Sensitivity

At Showell, data is categorized into four main classifications: Public, Internal Use, Confidential, and Restricted. Employees uncertain about the classification of any information asset should consult their direct manager or the CISO. The proper way to allow access, protect, distribute, and dispose of the information belonging to the various sensitivity levels can be found in the “Data Classification Policy”.

- **Public data:** This category includes data that is openly accessible, such as website content. It requires no additional control due to its public nature.
- **Internal Use:** This refers to company-wide data that should be protected but has minimal business impact if disclosed. Examples include internal policies, knowledgebase, and internal communications.
- **Confidential data:** This type of data is intended for use within the organization and includes materials like marketing strategies, pricing, and contact details. Unauthorized disclosure could negatively affect the company's reputation and profitability.
- **Restricted data:** Highly sensitive and usually protected by NDAs, this data is accessible only on a need-to-know basis. Trade secrets, intellectual property, personal data, financial details, health information, or customer data fall under this category. Disclosure could lead to significant financial or legal consequences.

Access control

Access to Showell information assets is restricted and will be granted to Showell employees and contractors to fulfill their duties on a need-to-use basis. Showell employees and contractors will not be granted access to any information asset that is not directly needed to their work in Showell with consideration to segregation of duties. Showell has defined various user roles, according to the various positions and activities in the company. Each Showell employee and contractor will be assigned one of these roles and receive access control privileges relevant to that role. Access requests need to be considered and approved by the Asset Owner before access provisioning.

Further information regarding access control can be found in the "Access Control policy".

User account management

Each employee at Showell has a personal user account for each system they need to access. This user account is personal and sharing it with others is not allowed.

Shared accounts (accounts that do not belong to a specific user, but rather serve a group of users) are not generally acceptable (unless necessary to carry out a specific task), as they prevent accountability for actions performed under that account. In case shared accounts are critical to the operation, they should be documented and approved by the Asset Owner.

User authentication

Logging into Showell's systems requires the users to authenticate themselves. The authentication method used depends on the sensitivity of the data, the authorization level requested by the user (e.g. regular user, administrator), and the access method used (e.g. internal network, remote access). Company-provided Single-Sign-On (SSO) and/or Multi-factor Authentication (MFA) should be used always when it is available.

Audit Trail

The use and activity of Showell assets are logged for audit trail. The logged data is audited for security and non-compliance with Showell's information security policy and additional procedures.

Acceptable use

The use of Showell's network, devices, software, hardware, email, and other communications channels and messaging systems are subject to Showell's acceptable use policy. Any use of external systems to process or transmit Showell information is subject to this information security policy and the acceptable use policy. All new and existing users should be aware of the acceptable use policy and accept it before using Showell's network, assets, and systems.

Further information regarding acceptable use can be found in the "Acceptable use policy".

Accountability

Each Showell user is personally accountable for his/her actions regarding access and use of Showell information assets. Anyone who will not comply with this policy shall be personally responsible for this non-compliance and subjected to sanctions elaborated in the Code of Conduct and as the law permits.

Communication Security

Showell employs communication security measures to safeguard its network, data, and assets. This comprehensive approach encompasses perimeter protection, network segregation, controlled external access, secure external communications, and restricted remote access.

- **Perimeter Protection:** Utilizing a combination of firewalls, routers, and security groups, Showell's perimeter defense effectively blocks unauthorized external access to different systems and prevents data leakage.
- **Limited External Access:** Access by external entities to Showell's assets is strictly controlled and pre-approved by the CISO.
- **Secure External Communications:** Communications over external channels (like the Internet), especially those involving confidential information, are encrypted using standard technologies.

- **Remote Access Protocol:** Remote access to our networks is restricted to a select group of employees who require it for their duties. This access is limited to essential services and data and is secured using VPN technologies.

Cryptography

Showell's Encryption Key Management Policy ensures data protection through secure encryption and key management practices.

- **Data Protection:** Encryption is used for data in transit and sensitive data at rest, using methods like VPN, TLS/SSL, and full disk or column/cell-level encryption.
- **Encryption:** We use SSL/TLS encryption with a minimum of 256-bit keys for data in transit and AES-256 for data at rest. Authentication information is encrypted with SHA2 standards.
- **Key Management:** Key practices include ensuring appropriate length, secure storage, and random generation. Keys are rotated periodically and destroyed securely when no longer needed. In case of compromise, keys are immediately replaced, and data is re-encrypted.

Compliance with this policy is required for all Showell employees, under the oversight of the CISO, who also maintains and reviews the policy document. For additional information regarding the cryptographic usage policy, refer to the Encryption Key Management Policy.

Disaster Recovery

Showell's Disaster Recovery Policy lays the foundation for our comprehensive Disaster Recovery Plan. This plan is instrumental in guiding our response to potential disruptions and in efforts to mitigate their impact. It details the recovery objectives, outlines the structure for its implementation, specifies mitigation measures, and describes the communication process for keeping staff, partners, and the public informed about changes to service delivery during a disaster. For more in-depth information on business continuity, please refer to the "Disaster Recovery Policy."

Change Management

Showell's operational environment and services are dynamic, to support the changing needs of its customers and the ever-growing requirement for capacity and performance. Our Change Management Policy efficiently manages technological changes to minimize operational disruptions and maintain security. This comprehensive policy applies to all employees and all technological assets.

We categorize changes as significant system changes, which undergo a detailed process including documentation and authorization, and minor updates managed directly by Asset Owners with proper documentation.

All Showell employees are responsible for complying with this policy, overseen by the CISO. The process encompasses everything from initiation to verification of changes, with simpler procedures for less impactful changes.

The change management process is described fully in the "Change Management policy".

Risk Assessment

The Company is committed to an ongoing process of risk assessment to ensure the continuous protection of its information systems. This involves a systematic approach to evaluating potential risks, factoring in the criticality of the systems, efficiency, cost, and practical feasibility of protective measures. Annually, a comprehensive risk assessment is conducted on all critical information systems to identify, quantify, and prioritize risks according to established criteria for acceptable risk levels.

Key aspects of our risk assessment process include:

- **Change-Driven Assessments:** Whenever changes affecting information security and privacy are implemented, risk assessments are conducted to understand the implications.
- **Data Protection Impact Assessment (DPIA):** In cases where new technologies or software may pose high privacy risks, a DPIA is carried out to assess the impact on personal data protection.

- **Risk Treatment and Management:** After assessing risks, appropriate information security risk treatment options are selected. This involves determining necessary controls and formulating a risk treatment plan, which is then subject to approval by risk owners and acceptance of any residual risks. All risk management activities are conducted in accordance with criteria set by the CISO.

Risk Treatment

The Chief Information Security Officer (CISO) at Showell is entrusted with overseeing security controls across all assets, locations, employees, and risk management processes. A key component of this responsibility is the development of a risk treatment plan. This plan outlines the resources, responsibilities, and priorities for addressing identified risks, and it is periodically reviewed and updated by the CISO.

Essential steps in the risk treatment process include:

- **Development of the Plan:** The risk treatment plan details both technology and process controls to be implemented. Once developed, it is presented to the Management team for approval.
- **Management Review and Approval:** Senior management reviews the proposed solutions, including steps to mitigate specific risks, and approves the treatment plan.
- **Implementation and Knowledge:** The IT & Security Team is equipped with the necessary knowledge to effectively implement and maintain these controls.
- **Cross-Departmental Collaboration:** The IT & Security Team leads ISMS operations with support from other departments, such as HR. Detailed roles and responsibilities are outlined in the “Roles and Responsibilities Policy”.
- **Effectiveness Measurement:** The effectiveness of security controls is regularly measured. This involves analyzing logs and records, including incident reports, access logs, network logs, Business Continuity tests, formal risk assessments, and penetration tests as per the annual work plan.
- **Statement of Applicability (SOA):** The SOA for the ISMS and PIMS implementation is prepared and approved by the CISO. This statement includes a list of controls as per ISO 27001 standards, their applicability, implementation status, and reasons for their selection or omission.

Malware Detection and Response

This procedure defines the process for detecting and responding to viruses, trojans, malware, and ransomware in Showell's devices and production systems. Further information can be found in the "System and Network Management policy".

Service Disruption Communication

This process defines the communication procedure for service disruption incidents. The process is designed to achieve the following goals in case of critical Service Disruption incidents:

- Provide near-instant initial notification to impacted customers and internal stakeholders.
- Ensure an ongoing communication channel as long as corrective measures are being taken.
- Deliver a clear postmortem analysis to customers and internal stakeholders following the resolution of the incident.

Further information regarding service disruption communication can be found in the "Incident Management policy".

Penetration and vulnerability tests

Showell conducts annual penetration testing to proactively identify and address security vulnerabilities. The process includes several key steps and measures:

- **Remediation of Critical/High Issues:** Any critical or high-severity issues identified during penetration tests are remediated promptly.
- **Re-Testing:** Following remediation, a re-test is conducted to verify that the critical and high issues have been effectively resolved.
- **Source Code Analysis:** Before deploying any code to production, it undergoes thorough source code analysis. This includes testing in a staging environment using a combination of automated and manual testing methods.

- **OWASP Compliance:** Tests are aligned with the Open Web Application Security Project (OWASP) standards to ensure comprehensive security coverage.
- **Continuous Monitoring:** A robust monitoring system is in place to continuously detect vulnerabilities, bugs, and potential system breakdowns. This system provides timely alerts to prevent security breaches.

These practices are integral to maintaining Showell's cybersecurity and ensuring the integrity and reliability of our systems.

Patch Management

We've implemented a patch management process to guarantee that all patches and updates undergo thorough testing before they are deployed and installed. For detailed guidelines and procedures, please refer to the Vulnerability and Patch Management Procedure.

Security Awareness and Training

Managers shall ensure that staff and external parties who are working with systems and data are formally aware of, and educated about, the security and privacy policies and procedures with which they must comply. This step is fundamental to establishing individual accountability.

All users within the scope of this document shall receive appropriate awareness and training and regular updates about Showell policies and procedures, as relevant for their job function. Security awareness is a key factor in maintaining a high level of information security in Showell. Each employee receives an information security briefing upon commencing work in Showell. The CISO together with the IT & Security Team and HR provides Showell employees with security awareness materials and training on an annual basis.

The CISO may also notify Showell employees when information security incidents that have a major impact on its products and services have occurred. These case studies are used to provide a better understanding of information security and enhance the security level of future software versions. Further information regarding Security Awareness and Training can be found in the "Security Awareness and Training policy".

Human Resources Security

All employee candidates go through pre-employment reference and/or background checks, according to the HR policy. New employees must sign an NDA agreement, and accept the Code of Conduct, and Acceptable Use policy when their work starts.

Changes in an employee's positions in Showell or change in their access privileges are reported to the direct supervisor and HR and IT & Security Team.

Termination of an employee's employment is reported to the direct supervisor, HR, and IT & Security Team who verifies that all of the employee's access privileges and authentication data have been revoked, relevant documentation signed and all assets returned.

Supplier Relationships

Showell diligently ensures that partners, suppliers, and contractors adhere to stringent security measures to protect both Showell's and its customers' information. This includes binding agreements and periodic audits. Before contractual commitments, we conduct third-party security assessments to safeguard our assets. Our CISO and Security team oversees compliance with Service Level Agreements, Codes of Conduct, Non-disclosure Agreements, and relevant security and privacy policies, especially if external parties gain access to our information or facilities. Regular risk assessments of all suppliers are conducted.

For detailed guidelines on third-party security, please refer to our Third Party Security Policy. The Physical Security Policy covers aspects related to physical control processes.

Information Sharing

We have defined, developed, and implemented secure information-sharing processes within the organization (with internal parties) and outside the organization (with external parties).

Software Development Security

Showell's Software Development Lifecycle (SDLC) Policy focuses on secure, agile, and efficient development practices, particularly suited to our startup environment. Key Elements of the policy are:

- **Agile Development Focus:** Our SDLC prioritizes the rapid development of Minimum Viable Products (MVPs), responsive to business and customer needs. This agile approach balances speedy product delivery with essential security considerations.
- **Secure Design and Coding:** Security is a core aspect of our development process, encompassing secure design, coding practices, and implementation. We emphasize regular security training for developers, including best practices in secure coding and the use of static analysis tools.
- **Risk Management:** The Chief Technology Officer (CTO) plays a pivotal role in identifying and managing risks throughout the development cycle, especially when introducing new interfaces, platforms, data items, or technologies.
- **Product Design and Development:** Design documents guide the development process, with a focus on security, serviceability, maintainability, scalability, performance, stability, fault tolerance, deployment flexibility, and testability.
- **Code Review and Change Management:** Security code reviews are integral, especially for sensitive system components. Our source code management practices, utilizing tools like Git and GitHub, ensure thorough review and tracking of changes.
- **Software Testing and Maintenance:** Testing follows QA procedures and includes sanity and performance checks. Maintenance includes monitoring for vulnerabilities in third-party tools and system changes.
- **Emergency Changes and Deployment:** Emergency changes are managed efficiently, with a post-implementation review. Deployments, primarily SaaS-based, ensure secure delivery and installation of updates.

The CTO is responsible for the SDLC Policy, ensuring its continuous review and accessibility to all staff. Showell's Software Development Security practices ensure that our products are not only innovative and responsive to market needs but also secure and reliable.

Security Incident Management and Reporting

Showell ensures that all employees work to prevent information security incidents from occurring. Should an incident occur, the company will swiftly implement appropriate actions. All employees, contractors, and third-party users are trained to be aware of the procedures for reporting the different types of security or privacy incidents, or vulnerabilities that might have an impact on the security of the company's assets. Information security incidents and vulnerabilities shall be reported as soon as possible.

Incident Reporting

Each security-related event (incident) that is detected by any Showell employee or system is reported to the relevant information asset owner, to the IT & Security Team, and to the CISO. The CISO compiles annual reports of information security activity and information security events and presents them to the Security Steering Committee when it convenes.

Reporting Privacy Breaches

In the event of privacy breaches that have exposed or damaged personal information, the proper authorities will be notified within 72 hours of Showell becoming aware of them. If privacy breaches carry a high risk of harm to data subjects, the data subjects will be notified without undue delay. Information security incidents and discovery of vulnerabilities associated with information systems shall be communicated promptly. Appropriate corrective actions shall be taken and formal incident reporting and escalation shall be implemented.

Incident Response

Security incidents detected by Showell employees, clients, or business partners are reported to the CISO and IT & Security Team. Together with relevant other personnel, they will perform the required forensics, mitigation, and improvement activities for each security incident. The CISO reports all security incidents and the lessons learned from them to the Security Steering Committee.

If a follow-up action against a person or company following an information security incident involves legal action (either civil or criminal), evidence is collected, retained, and presented to conform to the rules of evidence laid down in the relevant jurisdiction(s). Depending upon the type of security incident, the physical or technical evidence shall be retained for future legal purposes and provided to the operational people for further course of action. Further information regarding service disruption communication can be found in the "Incident Management policy".

Document Ownership

The CISO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with Showell's review requirements. A current version of this document is available to all members of staff on the company Intranet.