Information Security Policy

Doorway

SOC 2 Criteria: CC1.2, CC1.3, CC2.1, CC5.1, CC5.2, CC5.3
ISO 27001 Requirements: 6.2
ISO 27001 Annex A: A.5.1.1, A.6.1.5, A.6.2.1, A.6.2.2, A.7.1.2, A.7.2.2, A.7.2.3, A.7.3.1, A.11.2.8, A.11.2.9, A.12.6.1, A.18.1.2

Keywords: Corrective action, Security training, Clean desk

Purpose

Doorway's Information Security Policy has been developed to: establish a general approach to information security and the minimization of information misuse, compromise or loss; document security processes and measures; uphold ethical standards and meet the company's regulatory, legal, contractual, and other obligations; control business risk; and ensure that the appropriate company image and reputation is presented.

Scope

This policy applies to:

- Information in any form, regardless of the media on which it is stored, as well as, any facility, system, or network used to store, process, and/or transfer information.
- All Doorway employees, temporary staff, partners, contractors, vendors, suppliers, and any other person (collectively also referred to as "Staff" or "Personnel") or entity that accesses the company's networks or any other public or private network through company's networks or systems.
- All activity while using or accessing the company's information or information processing, storage, or transmission equipment, while on the company premises (owned, rented, leased, or borrowed) or remotely.
- Information resources that have been entrusted to the company by any entity external to the company (i.e. Customers, Staff, and others).
- Documents, messages, and other communications created on or communicated via the company systems are considered the company's business records and, as such, are

subject to review by third parties in relation to audits, litigation, process improvement, and compliance.

Background

This policy is the overarching policy over the rest of the security policies, which make up the Doorway's information security program (ISP). The series of security policies includes:

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity/Disaster Recovery Plans
- Code of Conduct
- Data Classification, Deletion, and Protection Policies
- Encryption and Password Policies
- Incident Response Plan
- Physical Security Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- Software Development Life Cycle Policy
- System Access Management Policy
- Vendor Management Policy
- Vulnerability Management Policy

Information Security Objectives

It is the policy of Doorway that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life-cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information. Ultimately, the information security goal of Doorway is to maintain:

- Confidentiality: data and information are protected from unauthorised access
- Integrity: Data is intact, complete and accurate
- Availability: IT systems are available when needed

Doorway’s information security objectives, consistent with the company’s information security program are:

- To protect information from all internal, external, deliberate, or accidental threats;
- To enable secure information sharing;
- To encourage consistent and professional use of information;

- To ensure clarity about roles and responsibilities associated with protecting information;
- To ensure business continuity and minimise business damage; and,
- To protect the company from legal liability and the inappropriate use of information.

Roles and Responsibilities

The Security Officer/CISO is responsible for:

1. The design, development, maintenance, dissemination, and enforcement of the items contained in this policy and other ISP policies.
2. Reporting on the performance of the information security program to top management.

The objectives and measures outlined by the ISP policies shall be maintained and enforced by the roles and responsibilities specified in each policy and the company *Skills Matrix*.

Policy Review

At minimum on an annual basis, a security and/or compliance committee composed of senior management and key personnel must discuss, evaluate and document the company’s ISP, ensuring strategic goals and objectives are continually being developed.

At a minimum on an annual basis, all ISP policies must be reviewed, modified and/or edited to meet necessary security standards. All policies must be signed and approved by authorized personnel.

Accessibility

Policies and/or procedures must be accessible to employees for review at all times via the compliance automation SaaS, Drata. Policies pertaining to positions must be reviewed and signed upon hire and on an annual basis by all employees.

Exceptions

Requests for any exceptions to any policies included within the ISP must be approved by Doorway’s Executive Management~~.~~ after proper review. Any approved exceptions will be reviewed annually.

Policy

Training

Management shall ensure that employees, contractors and third party users:

- Are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems;
- Are provided with guidelines which state security expectations of their role within the organisation;
- Are motivated and comply with the security policies of the organisation;
- Achieve a level of awareness on security relevant to their roles and responsibilities within the organisation;
- Conform to the terms and conditions of employment, which includes the organisation's information security policy and appropriate methods of working.

All new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter. New hire onboarding will be completed within 30 days after the date the employee or contractor is hired. Ongoing training will include security and privacy requirements as well as training in the correct use of information assets and facilities.

Additional specialised training will be required for individuals responsible for maintaining system security. Specialised topics would include spam, phishing, OWASP Top Ten list, and SANS Top 25 list. In addition, consistent with assigned roles and responsibilities, incident response and contingency training to personnel will be done:

- within 90 days of assuming an incident response role or responsibility;
- as required by information system or policy changes; and
- annually

The organisation will properly document that the training has been provided to all employees.

All employees are required to acknowledge in writing their understanding of the Information Security Program which includes a Code of Conduct upon hire and annually thereafter.

Clean Desk/Work Area Policy

Authorised users will ensure that all sensitive/confidential materials, hardcopy or electronic, are removed from their workspace and locked away when the items are not in use or an employee leaves his/her workstation. This will also increase awareness about protecting sensitive information. As such:

- Employees are required to ensure that all sensitive/confidential information, hardcopy or electronic, is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when the workspace is not in use, and must be shut down completely at the end of the day.
- Sensitive information must be removed from the desk and securely stored when the desk is unattended, and at the end of the day.
- Laptops and other portable computing devices must be properly stored/secured.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Treat mass storage devices such as external hard drives or USB drives as sensitive and always secure and encrypt them.
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Internet/Intranet Access and Use

Use of Doorway computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited "spam" that is unrelated to legitimate Company purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms;
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorisation from someone with the right to make such a grant;
- Making unauthorised copies of Company files or other Company data;
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorised users of Company systems;
- Misrepresenting oneself or the Company;

- Violating the laws and regulations of federal, state, city, province, or local jurisdictions in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Such access will be discontinued upon termination of employment, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer, the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

Teleworking

Requirements:

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. Refer to the *Encryption Policy* and the *Password Policy* for further information.
- Authorised Users must protect their login and password, without exception.
- While using a Doorway-owned computer to remotely connect to the company''s network, authorised users must ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorised user or third party.
- The most up-to-date antivirus software must be used on all computers. Third party connections must comply with requirements as stated in the Vendor Management Agreement.
- Equipment used to connect to Doorway's networks must meet the requirements for remote access and device use as stated in the *Acceptable Use Policy*, *Asset Management Policy*, and *System Access Control Policy*.

Remote Access Tools:

All remote access tools used to communicate between Doorway assets and other systems must comply with the following policy requirements:

- Multi-factor authentication (such as authentication tokens and smart cards that require an additional PIN or password) is required for all remote access tools
- The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
- Remote access tools must support the Doorway application layer proxy rather than direct connections through the perimeter firewall(s).
- Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the *Encryption Policy*.
- All antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

Mobile Endpoint and Storage Devices

Protecting endpoint devices issued by Doorway or storing company data is the responsibility of every employee. This pertains to all devices that connect to the company network, regardless of ownership. Mobile endpoint and storage devices are defined to include: desktop systems (in telework environment), laptops, PDAs, mobile phones, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or Doorway owned. An inventory of company-owned assets will be properly maintained.

For endpoint devices:

- Company-issued mobile devices will have antivirus and endpoint security pre-installed.
- Users must run an online malware scanner at least once a month.
- If browser add-ons are approved and installed, a browser testing tool shall be ran to ensure the security of the add-on.
- Mobile endpoint devices must further meet the requirements for use as stated in the *Acceptable Use Policy* and *Asset Management Policy*.

For storage devices:

- A risk analysis will be conducted prior to the use or connection to the company network, unless previously approved.
- Detection of incidents must immediately be reported to the Security Officer.
- Stolen mobile devices must immediately be reported to the Security Officer.

Intellectual Property Rights

Doorway takes handling and safeguarding of intellectual property very seriously. Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licenses.

To ensure this the following procedures will be maintained:

- Software will only be acquired through known and reputable sources, to ensure that copyright is not violated.
- An asset inventory will identify all assets with requirements to protect intellectual property rights.
- Proof and evidence of ownership of licenses, master disks, manuals, etc. will be maintained.
- Review of the asset inventory will also make sure that only software and licensed products are installed.
- Will ensure compliance with terms and conditions for software and information obtained from public networks

Information Security Requirements Analysis & Specifications

Doorway will identify its information security requirements through utilising different methods, ensure the results of the identification are documented and reviewed by all stakeholders, and will integrate the requirements and associated processes in early stages of projects.

- Methods
    - Policies and regulations
    - Threat modelling
    - Incident reviews
    - Use of vulnerability thresholds
- Factors
    - Level of confidence required towards the claimed identity of users, in order to derive user authentication requirements.
    - Access provisioning and authorisation processes, for business and privileged or technical users.
    - Informing users and operators of their duties and responsibilities.
    - Protection needs of assets, especially in terms of availability, confidentiality, integrity.
    - Business processes (e.g., transaction logging and monitoring, non-repudiation requirements).
    - Other security controls (e.g. interfaces to logging and monitoring or data leakage detection systems).

Employment Terms and Conditions

The following terms and conditions of employment at Doorway are the contractual obligations for employees or contractors for the safeguarding of information. They include, but are not limited to:

- Signing a confidentiality or non-disclosure agreement (NDA) prior to access to confidential information and processing facilities.
- Legal responsibilities and rights, particularly concerning intellectual property.
- Responsibilities for the classification of information and management of organisational assets associated with information, information processing facilities and information services handled by an employee or contractor.
- Responsibilities for handling of information received from third parties.
- Reviewing and agreeing with the security policies of the company.
- Duration of responsibilities beyond end of employment.
- Actions to be taken for non-compliance with the terms and conditions, and the company's security policies.

Disciplinary Process

Doorway's discipline policy and procedures are designed to provide a structured corrective action process to improve and prevent a recurrence of undesirable employee behaviour and performance issues. It has been designed to be consistent with Doorway cultural values, Human Resources (HR) best practices, and employment laws.

Doorway reserves the right to combine or skip steps depending on the facts of each situation and the nature of the offence. The level of disciplinary intervention may also vary. Some of the factors that will be considered are whether the offence is repeated despite coaching, counselling, or training, the employee's work record, and the impact the conduct and performance issues have on the organisation.

Step 1: Verbal Warning and Counselling

This initial step creates an opportunity for the immediate supervisor to schedule a meeting with an employee to bring attention to an existing performance, conduct or attendance issue. The supervisor should discuss with the employee the nature of the problem or the violation of company policies and procedures. The supervisor is expected to clearly describe expectations and the steps the employee must take to improve performance or resolve the problem.

Step 2: Formal Written Warning

If the employee does not promptly correct any performance, conduct or attendance issues that were identified in Step 1, a written warning will become formal documentation of the performance, conduct, or attendance issues and consequences. The employee will sign a copy of the document to acknowledge receipt and understanding of the formal warning. During Step 2, the immediate supervisor and HR representative will meet with the employee to review any additional incidents or information about the performance, conduct or attendance issues as well as any prior relevant corrective action plans. Management will outline the consequences for the employee of his or her continued failure to meet performance or conduct expectations.

A formal performance improvement plan (PIP) requiring the employee's immediate and sustained corrective action will be issued after a Step 2 meeting. A warning outlining that the employee may be subject to additional discipline up to and including termination if immediate and sustained corrective action is not taken may also be included in the written warning.

Step 3: Suspension and Final Written Warning

There may be performance, conduct, or safety incidents so problematic and harmful that the most effective action may be the temporary removal of the employee from the workplace. When immediate action is necessary to ensure the safety of the employee or others, the immediate supervisor may suspend the employee pending the results of an investigation. Suspensions that are recommended as part of the normal progression of this progressive discipline policy and procedure are subject to approval from a next-level manager and HR.

Step 4: Recommendation for Termination of Employment

The last step in the progressive discipline procedure is a recommendation to terminate employment. Generally, Doorway will try to exercise the progressive nature of this policy by first providing warnings, a final written warning or suspension from the workplace before proceeding to a recommendation to terminate employment. However, Doorway reserves the right to combine and skip steps depending on the circumstances of each situation and the nature of the offence. Furthermore, employees may be terminated without prior notice or disciplinary action.

Management's recommendation to terminate employment must be approved by HR and the supervisor's immediate manager. Final approval may be required from the CEO.

Performance and Conduct Issues Not Subject to Progressive Discipline

Behaviour that is illegal is not subject to progressive discipline, and such behaviour may be reported to local law enforcement authorities. Theft, substance abuse, intoxication, fighting and other acts of violence at work are grounds for immediate termination.

Enforcement

Doorway Management, under the explicit authority granted by the company CEO, retains the authority and responsibility to monitor and enforce compliance with this Policy and other policies, standards, procedures, and guidelines. Monitoring activities may be conducted on an on-going basis or on a random basis whenever deemed necessary by Management and may require investigating the use of the Company's information resources. The company reserves the right to review any and all communications and activities without notice.

Doorway will take appropriate precautions to ensure that monitoring activities are limited to the extent necessary to determine whether the communications or activities are in violation of Company policies, standards, procedures, and guidelines or in accordance with normal business processing performance or quality activities.

Violation of the controls established in this Policy is prohibited and will be appropriately addressed. Disciplinary actions for violations may include verbal and/or written warnings, suspension, termination, and/or other legal remedies and will be consistent with our published HR standards and practices.

Revision History

Version	Date	Editor	Description of Changes
1.0	24.02.2022	Henry Sinclair	Initial Creation