Data Protection Policy

Doorway

SOC 2 Criteria: CC6.1, CC6.7
ISO 27001 Annex A: A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.12.1.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.1, A.13.2.2, A.13.2.3, A.18.1.3

Keywords: Data encryption at rest, Data encryption in transit, Data separation, Cloud monitoring

---

Background

Doorway takes the confidentiality and integrity of its customer data very seriously and strives to assure data is protected from unauthorized access and is available when needed.

Purpose

This policy outlines many of the procedures and technical controls in support of data protection.

Scope

Production systems that create, receive, store, or transmit Doorway customer data (hereafter "Production Systems") must follow the requirements and guidelines described in this policy.

Roles and Responsibilities

The Security Officer is responsible for updating, reviewing, and maintaining this policy.

Policy

Doorway policy requires that:

- Data must be handled and protected according to its classification requirements and following approved encryption standards, if applicable.
- Whenever possible, store data of the same classification in a given data repository and avoid mixing sensitive and non-sensitive data in the same repository. Security controls, including authentication, authorisation, data encryption, and auditing, should be applied according to the highest classification of data in a given repository.
- Employees shall not have direct administrative access to production data during normal business operations. Exceptions include emergency operations such as forensic analysis and manual disaster recovery.
- All Production Systems must disable services that are not required to achieve the business purpose or function of the system.
- All access to Production Systems must be logged.
- All Production Systems must have security monitoring enabled, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, as applicable.

Data Protection Implementation and Processes

Customer Data Protection

Doorway hosts on Heroku in the EU region by default.

All Doorway employees adhere to the following processes to reduce the risk of compromising Production Data:

- Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
- Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
- Ensure Doorway Customer Production Data is segmented and only accessible to Customer authorised to access data.
- All Production Data at rest is stored on encrypted volumes using encryption keys managed by Doorway.
- Volume encryption keys and machines that generate volume encryption keys are protected from unauthorised access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
- Doorway is granted read-only access to all integrations with human resource platforms in order for customers to maintain data integrity.

Access

Doorway employee access to production is guarded by an approval process and by default is disabled. When access is approved, temporary access is granted that allows access to production. Production access is reviewed by the security team on a case by case basis.

Separation

Customer data is logically separated at the database/datastore level using a unique identifier for the

customer. The separation is enforced at the API layer where the client must authenticate with a chosen account and then the customer unique identifier is included in the access token and used by the API to restrict access to data to the account. All database/datastore queries then include the account identifier.

Monitoring

Doorway uses Sentry and Logtail to monitor the entire cloud service operation. If a system failure and alarm is triggered, key personnel are notified by text, chat, and/or email message in order to take appropriate corrective action.

Doorway uses a security agent to monitor production systems. The agents monitor system activities, generate alerts on suspicious activities and report on vulnerability findings to a centralised management console.

Confidentiality/Non-Disclosure Agreement (NDA)

Doorway uses confidentiality or non-disclosure agreements to protect confidential information using legally enforceable terms. NDAs are applicable to both internal and external parties. NDAs will have the following elements:

- Definition of the information to be protected
- Duration of the agreement
- Required actions upon termination of agreement
- Responsibilities and actions to avoid unauthorised disclosure
- Ownership of information, trade secrets and intellectual property
- Permitted use of the confidential information and rights to use information
- Audit and monitor activities that involve confidential information
- Process of notification and reporting of unauthorised disclosure or information leakage
- Information return or destruction terms when agreement is terminated
- Actions in case of breach of agreement
- Periodic review

Data At Rest

Encryption

All databases, data stores, and file systems are encrypted according to Doorway's *Encryption Policy*.

Retention

Stored data must be properly categorised and a retention schedule applied accordingly in conjunction with Doorway's *Asset Management Policy*, *Data Classification Policy* and *Data Deletion Policy*. Considerations for retention timeframe include:

- Statutory, regulatory or contractual requirements
- Type of data (e.g., accounting records, database records, audit logs)
- Type of storage media (e.g., paper, hard drive, server)

Storage and Disposal

Stored data must be properly stored and handled while at rest. Considerations for storage and disposal of data at rest in conjunction with Doorway's *Asset Management Policy*, *Data Classification Policy* and *Data Deletion Policy* include:

- Authorisation to access or manage stored data
- Proper identification of records and their retention period
- Technology change and ability to access data throughout retention period
- Acceptable timeframe and format to retrieve data
- Appropriate methods of disposal

Data In Transit

Necessity

Data will only be transferred where strictly necessary for effective business processes.

Transfer Factors

Before choosing the method of data transfer, the following must be considered:

- Nature, sensitivity, confidentiality, and value of the information
- Size of data being transferred
- Impact of loss during transit

Encryption

To ensure the safety of data in transit:

- All external data transmission must be encrypted end-to-end using encryption keys managed by Doorway. This includes, but is not limited to, cloud infrastructure and third party vendors and 3rd party applications, including integrations with human resource platforms.
- All internet and intranet connections are encrypted and authenticated using a strong protocol, a strong key exchange, and a strong cipher.

End-user Messaging Channels

- Restricted and sensitive data is not allowed to be sent over electronic end-user messaging channels such as email or chat, unless end-to-end encryption is enabled.
- Messages must be protected from unauthorised access, modification or denial of service commensurate with the classification scheme adopted by the organisation.
- Messages must be reviewed prior to sending to ensure correct addressing and transportation of the message.
- The reliability and availability of the messaging channel must be verified.

- All applicable legal requirements will be adhered to.
- Use of external public services such as instant messaging, social networking or file sharing will require prior approval and authorisation.
- Publicly accessible networks will be controlled by stronger authentication.

Event Logs

All Doorway systems that handle confidential information, accept network connections, or make access control (authentication and authorisation) decisions will record and retain audit-logging information sufficient to answer: What activity was performed? Who performed it? Where, when, and how (with what tools) was it performed? And, what was the status, outcome, or result of the activity?

Logged Activities

The logs will be created whenever the system is asked to perform any of the following activities:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
- Create, update, or delete information not covered in above;
- Initiate a network connection;
- Accept a network connection;
- User authentication and authorisation for activities covered above such as user login and logout;
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
- Application process startup, shutdown, or restart;
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.
- A new connection is established between Doorway's API for human resource platform integrations.
- New data is imported via a human resource platform integration.

Log Elements

Each log will identify or contain at least the following elements, directly or indirectly (unambiguously inferred):

- Type of action – examples include authorise, create, read, update, delete, and accept network connection.
- Subsystem performing the action – examples include process or transaction name, process or transaction identifier.

- Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, MAC address, and API connection name. Note that such identifiers should be standardised in order to facilitate log correlation.
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, MAC address, and name of newly imported subject information. Note that such identifiers should be standardised in order to facilitate log correlation.
- Before and after values when action involves updating a data element, if feasible.
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
- Whether the action was allowed or denied by access-control mechanisms.
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

Formatting, Storage, Clock Synchronisation

- The system will support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document.
- The system will also ensure clock synchronisation for the accuracy of audit logs. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol will be used to keep all of the servers in synchronisation with the master clock.

Administrators and Operator Logs

To safeguard and prevent manipulation of logs by privileged users the following will be implemented where appropriate and possible:

- System administrators are not permitted to erase or de-activate logs of their own activities.
- Real-time copying of logs to a system outside the control of a system administrator or operator.
- Monitoring system and network administration activities by using an intrusion detection system managed outside of the control of system and network administrators.
- Frequent review of logs to maintain accountability of privileged users.

Revision History

Version	Date	Editor	Description of Changes

1.0	24.02.2022	Henry Sinclair	Initial Creation
2.0	13.10.2022	Hugh Fraser	Inclusion of HR integration specifications