Business Continuity Plan

Doorway

SOC 2 Criteria: CC5.3, CC7.5
ISO 27001 Annex A: A.17.1.1, A.17.1.2

Keywords: BIA, Status Page, Worksite Recovery

Purpose

This policy establishes procedures to recover Doorway following a disruption in conjunction with the *Disaster Recovery Plan.*

Policy

Doorway policy requires that:

- A plan and process for business continuity, including the backup and recovery of systems and data, must be defined and documented.
- The Business Continuity Plan shall be simulated and tested at least once a year. Metrics shall be measured and identified recovery enhancements shall be filed to improve the process.
- Security controls and requirements must be maintained during all Business Continuity Plan activities.

Roles and Responsibilities

This Policy is maintained by the Doorway Security Officer and Privacy Officer. All executive leadership shall be informed of any and all contingency events.

Line of Succession

The following order of succession ensures that decision-making authority for the Doorway Business Continuity Plan is uninterrupted. The CEO is responsible for ensuring the safety of personnel and the execution of procedures documented within this Plan. The Head of Engineering is responsible for the

recovery of Doorway technical environments. If the CEO or Head of Engineering is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Business Operations Lead shall function as that authority or choose an alternative delegate.

Response Teams and Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting Doorway infrastructure and systems.

1. DevOps is responsible for assuring all applications, web services, platforms, and their supporting infrastructure in the Cloud. The team is also responsible for testing re-deployments and assessing damage to the environment. The team leader is the Head of Engineering.
2. Security is responsible for assessing and responding to all cybersecurity related incidents according to Doorway Incident Response policy and procedures. The security team shall assist the above teams in recovery as needed in non-cybersecurity events. The team leader is the Security Officer.

Members of above teams must maintain local copies of the contact information of the Business Continuity Plan succession team. Additionally, the team leads must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

All executive leadership shall be informed of any and all contingency events.

Policy

Business Impact Analysis (BIA)

The BIA will help identify and prioritise system components by correlating them to the business processes that the system supports. It will allow for the characterisation of the impact on the processes if the system becomes unavailable. The BIA has three steps:

1. **Determine business processes and recovery criticality.** Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organisation can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

See Appendix A for the BIA breakdown.

Work Site Recovery

In the event a Doorway facility is not functioning due to a disaster, employees will work from home or locate to a secondary site with Internet access, until the physical recovery of the facility impacted is complete.

Doorway's software development organisation has the ability to work from any location with Internet access and does not require an office provided Internet connection.

APPENDIX A

Business Impact Analysis

System Description

Doorway's technology is a web-based software product that extends into Apple Wallet and Google Pay. The primary product offering is a digital business card that is native to digital wallets on the iOS and Android operating systems, and is managed via a web based interface or integration with a human resource platform. Doorway's operating environment is as a distributed team, located across Europe where its services are hosted also. Doorway's services are available globally, to serve an international customer base.

Doorway's web hosted application (found at https://app.doorway.io, and associated subdomains) provides key functionality for the creation, management, distribution, deletion, and payment of its digital business cards. The cards are added to the native digital wallets on iOS and Android, and provide a single primary function which is to efficiently share contact details about its bearer. This is achieved by scanning the QR code present on the digital business card. For recipient devices, no internet connection or specific mobile application is required in order to scan a Doorway digital business card or receive the inbound data.

All customer data is stored within the EU, and regular backups are captured to ensure roll back and restoration capabilities.

Data Collection

Data collection can be accomplished through individual/group interviews, workshops, email, questionnaires, or any combination of these.

Determine Process and System Criticality

Identify the specific business processes that depend on or support the information system, using input from users, managers, business process owners, and other internal or external points of contact.

BUSINESS PROCESS	DESCRIPTION
Software Services	The ability for Doorway's software engineers to build, fix, edit, and maintain the code repositories for the main application/platform and associated services.
DevOps	The ability for Doorway's software engineers to commit, test, review, and deploy fixes and improvements to the Doorway application/platform and associated services.
Design	The ability to design new User Interfaces and User Experiences.
Sales	The ability to conduct outbound sales activities such as emailing, telephone calls, and messaging to generate new customers and revenue.
Accounting	The ability to bookkeep Doorway's financial affairs, ensure financial compliance, handle all accounts & payments, and conduct all planning activities.
Marketing & Advertising	The ability to segment the market through research and conduct marketing activities such as digital ad campaigns and SEO.
Customer Support & Success	The ability to handle customer support requests, incidents, and ensure customers realise the full potential of Doorway's products and services.
Operations / IT	The ability to undertake all relevant organisation operational activities such as Risk Assessments and Account administration.
HR/People	The ability to manage employment arrangements with local and remote employees.

Outage Impacts

Impact categories and values characterise levels of severity to the company that would result for that particular impact category, if the business process could not be performed. These impact categories and values are samples and should be revised to reflect what is appropriate for the organisation.

BUSINESS PROCESS	IMPACT CATEGORY				
	SEVERE	HIGH	MEDIUM	LOW	NONE
Software Services	X				
DevOps	X				
Design				X	
Sales		X			

Accounting	X				
Marketing & Advertising			X		
Customer Support & Success	X				
Operations / IT	X				
HR / People		X			

Estimated Downtime

Downtime factors resulting from a disruptive event will be estimated by working directly with business process owners, departmental staff, managers, and other stakeholders. The following downtime categories will be considered:

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time managers are willing to accept for a business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on:
    1. Selection of an appropriate recovery method; and
    2. The depth of detail which will be required when developing recovery procedures, including their scope and content.
- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.
- **Recovery Point Objective (RPO).** The RPO represents the point in time, prior to a disruption or system outage, to which business process data must be recovered (given the most recent backup copy of the data) after an outage.

BUSINESS PROCESS	MTD	RTO	RPO
Software Services	3hrs	2hrs	±1hr
DevOps	6hrs	3hrs	±1.5hrs
Design	36hrs	12hrs	±1hr
Sales	12hrs	6hrs	±1hr
Accounting	72hrs	36hrs	±1hrs
Marketing & Advertising	72hrs	36hrs	±2hrs
Customer Support & Success	3hrs	1hr	±15mins
Operations / IT	3hrs	1.5hrs	±20mins
HR / People	36hrs	12hrs	±15mins

STEP 2. Identify Resource Requirements

Identify the resources that compose Doorway in support of business processes, including hardware, software, and other resources such as data files.

SYSTEM RESOURCE/ COMPONENT	PLATFORM/OS/ VERSION (AS APPLICABLE)	DESCRIPTION
Heroku (AWS)		Our infrastructure provider, where we host our application, database, and related services
AWS S3		Where we store media files needed to deliver Doorway's services to its customers. Primary files stored are Branding assets belonging to companies and .pkpass files for Apple Wallet users.
Github		Our Version Control provider.
Cloudflare		Our DNS proxy server and web application firewall.

STEP 3. Identify Recovery Priorities for System Resources

List the order of recovery for Doorway resources, and identify the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption. A system resource can be software, data files, servers, or other hardware and should be identified individually or as a logical group.

PRIORITY	SYSTEM RESOURCE/COMPONENT	RTO
Heroku (AWS)		±1hr
AWS S3		±1hr
Github		±1hr
CloudFlare		±1hr

Any alternate strategies in place to meet expected RTOs will be identified, including backup or spare equipment and vendor support contracts.

Revision History

Version	Date	Editor	Description of Changes
1.0	29/03/2022	Henry Sinclair	Initial Creation
2.0	18/07/22	Hugh Fraser	Policy Edit
3.0	26/07/22	Hugh Fraser	Policy Edit
4.0	13.10.2022	Hugh Fraser	Inclusion of HR platform integration specifications