



Information Security Business Continuity Plan

Document Control

Organisation	Pixel Fusion
Document Name	Information Security BCP
Version	1.0

Document Revision History

Date	Version	Changed By	Details of Change
25/11/2025	DRAFT	Alice Ward	Draft of Procedure
01/12/2025	1	Gareth Heggie	Approved

Statement of Applicability Controls

Control Reference	Control Name
5.2	Information Security Roles and Responsibilities
5.5	Contact With Authorities
5.24	Information Security Incident Management Planning and Preparation
5.29	Information Security During Disruption
5.30	ICT Readiness for Business Continuity
8.14	Redundancy of Information Processing Facilities

Contents

1. Purpose.....	4
2. Scope.....	4
3. Information Security BCP	4
3.1 Information Security Business Continuity Plan.....	4
3.2 Emergency Contacts	4
3.3 Incident Roles and Responsibilities	4
3.4 Business Function Recovery and Information Security Continuity Priorities....	5
3.5 Relocation Strategy	6
3.6 Regular Testing of Business Continuity.....	6
3.7 ICT Readiness For Business Continuity	6
4. Critical Functions and Recovery Priorities	7
5. Post-Incident Review	7
6. Document Compliance.....	7
6.1 Compliance Measurement.....	7
6.2 Exceptions.....	7
6.3 Non-Compliance.....	7
6.4 Continual Improvement	7

1. Purpose

This document's purpose is to ensure a consistent and efficient approach is followed and adopted during any Business Continuity Event which could affect the organisation negatively.

2. Scope

This document is aimed particularly at the individual roles listed later within this document, however, is still to be read by all users of Pixel Fusion's systems to ensure that when required all users can aid in investigatory procedures appropriately and stay compliant with all legal, contractual, and regulatory requirements.

3. Information Security BCP

3.1 Information Security Business Continuity Plan

This plan has been developed to ensure the organisation can continue to operate in the event of a disaster or major incident in relation to information security, or when an unrelated incident negatively impacts our information security stance.

This document provides clear and concise processes for the CISO or assigned Incident Commander to follow to continue organisational operations whilst recovery continues.

It is vital that all steps taken to adopt and follow the Business Continuity Plan are documented methodically for future reference and an audit trail of actions.

If the collection of evidence is required, then the **Collection of Evidence Procedure(s)** are to be strictly followed by all involved users.

3.2 Emergency Contacts

A list of emergency contacts who may be needed when the Information Security BCP is enacted.

Contact Details	Contact Number	Contact
CISO (Gareth Heggie)	0330 133 2536	Support
Information Commissioner's Office (ICO)	0303 123 1113	Support Line
Ambulance	999	Emergency
Fire	999	Emergency
Police	999	Emergency

3.3 Incident Roles and Responsibilities

The following roles and responsibilities are to be assumed during an incident.

Main Role	Incident Role	Incident Responsibilities
CISO	Incident Commander	Coordinate incident and lead recovery efforts.
Information Security Team Member	Backup Incident Commander	Assumes the roles and responsibilities of Incident Commander if the CISO is unavailable.

B&B if External DPO / Information Security Services are Applicable	Incident Advisor Information Security Advisor Data Protection Advisor	Advise the Incident Commander and Pixel Fusion as an organisation in the progress and coordination of recovery. Assess the security risk to the organisation caused by the incident. Ensure continuity of information security.
Other Pixel Fusion Employee	Narrative Coordinator	Narrate a timeline of events in real time during an incident. Collate evidence and information to create a timeline and chain of evidence.

The Narrative Coordinator role has not been allocated to an individual role within the organisation to ensure that there would be no conflict of interest on a per event basis.

The Narrative Coordinator will be selected by the Incident Commander on a per event basis, dependant on the availability and experience of employees.

It is the responsibility of the Narrative Coordinator to create a timeline which related to all remedial or reactive actions, not just those surrounding information security.

3.4 Business Function Recovery and Information Security Continuity Priorities

The following priorities have been established by the CISO. In a case where multiple priorities are compromised, the priority of recovery will be at the discretion of the Incident Commander:

- Restore internal communications;
- Restore external communications;
- Restore access to network and cloud storage;
- Activate redundancy components;
- Backup any data in use;
- Move to backup services if required;
- Test critical functionality, services, and risks to information security;
- Investigate cause of disaster;
- Investigate losses of services, assets, and profit;
- Investigate any security risks to the business caused by the incident;
- Create new safeguards and controls to information security; and
- Change the **Information Security BCP** as necessary.

3.5 Relocation Strategy

Organisational functions are primarily cloud and internet based, built with high redundancy and control within them. Should a situation arise where the main office is compromised due to infrastructure issues, legal, or an act of God, the following steps are to be taken:

- The Incident Commander will inform all relevant employees that the main office will be out of action with as much notice as reasonably practical, using the normal method of communication [MS Teams]. Where not possible due to the nature of the incident, employees will be informed using their contact details as provided by HR.
- Employees will relocate (if not already located at) to their remote working locations and will test access to systems and storage (unless instructed otherwise), assessing critical functions and network access.
- Employees will inform the Incident Commander that they have conducted either a successful or unsuccessful test.
- Once all required employees have communicated their results to the Incident Commander, and any issues resolved related to the communication results are solved, then the Incident Commander will inform all required employees (via MS Teams) that the communications have been tested and the backup working locations are now active.
- The Incident Commander will communicate with senior members of staff to restore normal working practices as soon as possible, and to assess any problems arising from the relocation.
- Once the incident has been rectified the Incident Commander will be responsible for communicating this to employees via MS Teams.
- Employees returning to the office will test their access to systems and storage and inform the Incident Commander on the result of the test.
- Once all tests have been successfully completed, the Incident Commander will communicate the end of the incident to all staff and stand down as the Incident Commander.
- Once the Incident Commander has stood down, normal operations will resume.

3.6 Regular Testing of Business Continuity

Regular tests of the Information Security BCP are conducted in line with the **Information Security Calendar**. The test results are then to be recorded by the responsible employee within the **BCP Test Record Log**.

3.7 ICT Readiness for Business Continuity

The availability of Pixel Fusion's information and other associated assets is tested on a regular basis as per the Information Security Calendar and recorded within the BCP Test Record Log.

Based on the outcome of the tests conducted, the CISO will add discovered risks to the Risk Register and any necessary organisational improvements to the Improvement Log.

4. Critical Functions and Recovery Priorities

Pixel Fusion maintains a list of critical functions and prioritises their recovery based on business impact. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are defined for each:

- Cloud-hosted applications: RTO = 4 hours, RPO = 1 hour
- Client data access and APIs: RTO = 8 hours, RPO = 4 hours
- Internal communication tools (e.g. email, Teams): RTO = 12 hours
- Development infrastructure: RTO = 24 hours.

5. Post-Incident Review

A formal post-incident review is carried out within 5 working days of a BCP event. The review includes:

- Root cause analysis
- Timeline of recovery actions
- Lessons learned and corrective actions
- Updates to the BCP and related policies.

6. Document Compliance

6.1 Compliance Measurement

The Information Security Team will verify compliance to this procedure through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

Any exception to the procedure must be approved and recorded by the CISO in advance and reported to the Information Security Team.

6.3 Non-Compliance

Security breaches by employees relating to the ISMS may be treated as misconduct as per the Disciplinary Procedure and serious breaches may lead to dismissal.

6.4 Continual Improvement

This document is updated and reviewed as part of the continual improvement process.