Disaster Recovery Policy (JICT)

1 JICT DISASTER RECOVERY POLICY OVERVIEW

1.1 About this Policy

This policy is for those providing and supporting ICT (Information Communication Technology) Services, including:

- Architecture & Strategy
- IaaS
- PaaS
- Business Partners
- Application Support
- Vendor Managers
- Third-Party Providers of IT Services (i.e. SaaS)

1.2 Rationale

This policy covers all Joint ICT services and infrastructure, both internal and external, which are provided for business purposes. This policy covers planning for the loss of any service or infrastructure which is caused by a disaster scenario. These scenarios include, but are not limited to,

- loss of internal data centres
- loss of 3rd Party SaaS Solutions
- cyber incidents

Disaster recovery planning ensures that in case of a disaster, there are defined, controlled processes to restore services, recover data, and complete investigative actions to produce lessons learned, and mitigate future risk of impact from similar events.

1.3 Legislation/National Standards (list)

- ITIL v4 Framework
- NIST SP 800-53 r5 (Cyber Security Framework)
- ISO 27001 (Information Security Standard)
- ISO 27031 (IT Disaster Recovery and Business Continuity)

1.4 Intention

The intention of this policy is to give Joint ICT staff and managers clear guidance on the creation and use of Disaster Recovery Plans.

1.5 General Principles

This policy applies equally to all Joint ICT staff and third-party providers of IT services to Thames Valley Police and Hampshire & Isle of Wight Constabulary, not only those assigned responsibilities to perform restoration of services. To ensure that IT services provided are protected, disaster recovery plans shall be documented using the guidance provided within this policy.

2 STATEMENT OF POLICY

This policy refers to Policy Statements, **POL.ITDR.001** to **POL.ITDR.014**. **POL.ITDR.XXX** shows the specific policy statement to be adhered to.

2.1 What is an IT disaster event?

An IT disaster event is any incident that causes actual or potential loss of availability or integrity of an JICT system, which results in the JICT system being unable to function during business as usual (BAU) operations.

2.2 What is IT disaster recovery?

IT disaster recovery is the planned response to a disaster event which will restore an JICT System to BAU operations.

2.3 IT Disaster Recovery Plan

An IT Disaster Recovery Plan lists the actions to be taken to recover an JICT System from a disaster event, together with a list of key roles and their responsibilities.

POL.ITDR.001: Each JICT system **shall** have an IT Disaster Recovery Plan.

2.4 Roles and Responsibilities

POL.ITDR.002: All Disaster Recovery Plans **shall** have an up-to-date list of roles and responsibilities. Each role **shall** have a name, with at least two sets of contact details.

POL.ITDR.003: All staff listed in a Disaster Recovery Plan must know their role and responsibilities. The list of roles and responsibilities **should** include internal and external stakeholders, together with everyone listed on the communications list. The list of roles and responsibilities **shall** align with the Major Incident Management Process.

Many individuals and teams may manage business and IT service continuity and escalation in case of a disaster.

These may include:

- Executive Committee
- Senior Information Risk Owner (SIRO)

- Information Asset Owner (IAO)
- Strategic Governance & Risk Management Leads in both forces
- Joint ICT Senior Management (SMT) and Extended Leadership (ELT)

A Disaster Recovery plan **should** include the relevant escalation process through the teams and individuals listed for each JICT system.

2.5 Planning

An IT Disaster Recovery Plan supports the decisions and steps taken to reduce the effects of disasters and shows the steps needed to recover JICT systems back to BAU.
An IT Disaster Recovery Plan **shall**:

- have named risk scenarios and strategies to recover from them.
- describe the circumstances in which the plan is invoked.

2.6 Business Impact Assessment

A Business Impact Assessment (BIA) **shall** be undertaken to find the key disaster recovery requirements of the assets, services, and business processes supported by a specific JICT system.

The BIA **should** have:

- a Maximum Tolerable Period of Disruption (MTPD): the maximum time that the services and/or systems may be disrupted or unavailable before the impact becomes unacceptable.
- a Minimum Business Continuity Objective (MBCO): the minimum level of services provided during a disaster.
- a Recovery Time Objective (RTO): the time between a disaster event occurring and full JICT Systems and services being restored.
- a Recovery Point Objective (RPO): the period during which the business can tolerate data loss.

POL.ITDR.004: A Disaster Recovery Plan **shall** have an **RTO** and **RPO**. The plan may have more than one of these depending on the systems involved.

POL.ITDR.005: Any disaster recovery action **shall** ensure that the JICT System can recover from a disaster within the RTO recorded in the BIA.

POL.ITDR.006: Any disaster recovery action **shall** ensure that the JICT System can recover from a disaster within the RPO recorded in the BIA.

2.7 Testing and Readiness Review

An IT Disaster Recovery Plan **shall** be tested regularly to ensure that:

- The plan is still fit for purpose.

- The plan reflects all changes in personnel and updates to system information.
- Everyone with a role in the plan knows their responsibilities.

POL.ITDR.007: Each JICT system **shall** have its IT Disaster Recovery Plan tested before starting live operations.

POL.ITDR.008: All IT Disaster Recovery Plans **shall** be tested at least annually, and after significant update to a JICT system. The testing schedule **shall** be outlined in the IT Disaster Recovery Plan.

POL.ITDR.009: The IT Disaster Recovery Plan **shall** be reviewed after each test and updated as needed to ensure it is fit for purpose.

POL.ITDR.010: Each IT Disaster Recovery Plan **shall** define the circumstances when the plan is to be invoked.

2.8 Reporting and Alerting

The reporting and alerting structure of an IT Disaster Recovery Plan **should** align with that of the corresponding IT Security Incident Response Plan.
Every stakeholder that needs to be informed **should** be listed as a key contact within the plan.

POL.ITDR.011: The reporting and alerting structure within an IT Disaster Recovery Plan **shall** align with the relevant IT Security Incident Management Plan and Business Continuity Plan. Responsibility for business continuity sits with the SO.

2.9 Recovery and Review

The process to recover from a disaster event **shall** ensure that security vulnerabilities are not introduced or re-introduced during the restoration process.

POL.ITDR.012: Each IT Disaster Recovery Plan **shall** have pre-defined and tested processes and procedures to restore an JICT system or services, which has been disrupted or disabled during a disaster event.

POL.ITDR.013: Each Disaster Recovery Plan **shall** describe in detail the procedures to enable a JICT Security System to return from recovery mode to BAU. Lessons learned **shall** be collated in an after-action report and be fed back to appropriate stakeholders.

POL.ITDR.014: Following a disaster incident, an after-action report **shall** be produced, which has:

- all lessons learned.
- actions to be taken to update processes and plans.

3 GOVERNANCE OF POLICY

This policy is governed by JICT Governance & Assurance team within the Process Assurance & Disaster Recovery Lead role. This policy will be reviewed on an annual basis. Failure to prepare disaster recovery plans for ICT services may result in detrimental impacts to provision of services in case of disasters. This may affect front-line policing and consequently impacts on public safety.

4 HEALTH AND SAFETY AT WORK

4.1 This policy is to be read in conjunction with the Force Health and Safety Management Policy and Health and Safety Manual, which set out the requirement for documented risk assessment by a competent person, when exposure to a particular hazard arising from workplace or pre-planned policing work activity can be said to be foreseeable.

4.2 The Health, Safety and Welfare issues connected with this policy include:

- The need for supervisors to check in with their officers and staff, and ensure they are properly supported should they be exposed to risk.

5 COMMUNICATIONS, CHALLENGES AND REPRESENTATIONS

5.1 Communication

This policy will be published in the Joint ICT Document Library and managers will inform staff of the new policy and any future updates. All staff will be directed to the policy in the document library.

5.2 Challenges and Representation

Any challenges to this policy or recommendations for amendment should be addressed to the Head of Governance & Assurance and the Process Assurance & Disaster Recovery Lead.

6 NEXT REVIEW DATE

16/12/2026

7 FREEDOM OF INFORMATION

Suitable for publication.

8 GOVERNMENT SECURITY CLASSIFICATION POLICY

Official