Essex County Council

Technology Services
IT Disaster Recovery Policy

Title	TS IT DR Policy
Author/Owner	TS Policy & Assurance Team
Status	LIVE
Version	1.11
Last reviewed	March 2021
Approved Date	April 2021
Approved By	Director of Technology Services
Next Review Date	April 2022
Security Classification	Official

Contents

1. Overview

IT Disaster Recovery (IT DR) is an area of security planning that aims to reduce the impact on Essex County Council (ECC) from the catastrophic loss of IT services. IT DR allows an organisation to maintain or quickly resume mission-critical functions following a disaster.

IT DR Management is based around the following key principles:

a) Incident Prevention - Protecting IT services from threats, such as environmental and hardware failures, operational errors, malicious attack, and natural disasters, is critical to maintaining the desired levels of systems availability for an organisation.
b) Incident Detection - Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service.
c) Response - Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimize any downtime. Reacting poorly can result in a minor incident escalating into something more serious.
d) Recovery - Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated at a later time or, in some circumstances, not at all; and
e) Improvement – Lessons learned from small and large incidents should be documented, analysed, and reviewed. Understanding these lessons will allow the organisation to better prepare, control and avoid incidents and disruption.

1.1 Outcomes and Benefits

The benefits of effective IT DR Management for ECC are that it:

a) Understands the risks to continuity of IT services and their vulnerabilities.
b) Identifies the potential impacts of disruption to IT services.
c) Develops and enhances competence in its IT staff by demonstrating credible responses through exercising IT continuity plans and testing IT DR arrangements.
d) Provides assurance to Senior Management that it can depend upon predetermined levels of IT services and receive adequate support and communications in the event of a disruption.
e) Provides assurance to top management that information security (confidentiality, integrity, and availability) is properly preserved, ensuring adherence to information security policies.

f) Provides additional confidence in the business continuity strategy through linking investment in IT solutions to business needs and ensuring that IT services are protected at an appropriate level given their importance to the organisation.
g) Has IT services that are cost-effective and not under or over-invested through an understanding of the level of its dependence on those IT services; and the nature, location, interdependence, and usage of components that make up the IT services.
h) Understands and documents stakeholders' expectations and their relationships with, and use of, IT services.

1.2 Objectives

This policy is implemented to minimise the impact of significant incidents on services and improve the ability to recover from the unavailability of IT systems to an acceptable level through a combination of planning, response, and recovery controls.

In order to achieve this, the following objectives are set out:

a) Identify critical systems and applications based on risk assessment.
b) Establish baseline recovery time capabilities and objectives for each impacted service.
c) Identify gaps between current and required capabilities for system recovery.
d) Incorporate disaster recovery capability into solution design and enterprise architecture.
e) Agree communication protocols for all activities concerned with management and user communications related to the disaster.
f) Develop and implement procedures and plans for critical business systems and applications to ensure timely resumption of essential services.
g) Implement regular reviews of IT DR policy, plans and processes at planned intervals and when significant changes occur, test the ongoing effectiveness and report outcomes to Senior Managers.

1.3 Scope

All staff and anyone undertaking work on behalf of the Council, including Members and volunteers are responsible for adhering to this policy.

This policy applies to services that are deemed critical to the business and have a defined Service Definition which states the level of required availability.

This policy applies to management of IT disaster recovery - a disaster being classified as a serious incident that cannot be managed within the scope of normal incident or major incident management processes.

The key elements of IT DR Management can be summarised as follows:

a) People: the specialists with appropriate skills and knowledge, and competent backup personnel.
b) Facilities: the physical environment in which IT resources are located.
c) Technology:
    1) hardware (including racks, servers, and storage arrays).
    2) network (including data connectivity and voice services), switches and routers; and
    3) software, including operating system and all application software.
d) Data: application data, voice data and other types of data.
e) Processes: including supporting documentation to describe the configuration of IT resources and enable the effective operation, recovery, and maintenance of IT services; and
f) Suppliers: other components of the end-to-end services where IT service provision is dependent upon an external service provider or another organisation within the supply chain, e.g. telecoms carrier or Internet service provider.

2. Responsibilities

The activities for Disaster Recovery Management involves collaboration between representatives from multiple teams within Technology Services with relevant roles and job functions. This co-ordination involves the collaboration of separate teams, which may include the following:

Chief of Operations (COO) – Overall accountability for Disaster Recovery Management within Technology Services.

Chief Technology Officer (CTO) – Responsible for ensuring DR is considered and included in technology solution designs.

IT DR Response Team – Comprised of COO (Chair), Major Incident Manager, Operational Team Leads, Policy & Assurance Team – responsible for all management activities following invocation of disaster recovery operations.

Policy & Assurance Team – Responsible for production and maintenance of the IT DR Policy, facilitating DR risk management, facilitation of DR planning and testing, and DR reporting to TSLT.

Platform & Infrastructure Team – Responsible for maintaining DR services, the production and ongoing maintenance of DR plans, processes, and procedures, and participating in DR test planning and execution.

Applications Teams - Responsible for maintaining DR services, the production and ongoing maintenance of DR plans, processes, and procedures, and participating in DR test planning and execution.

Service Operations Team - Responsible for working with Technology Assurance and Operations teams to implement arrangements for disaster recovery and documents recovery procedures in order to ensure a rapid recovery of business services reducing any adverse impact on business operations.

Emergency Planning & Resilience (EP&R) Team – Responsible for the co-ordination of the Business Continuity Management program across ECC including the provision of RTO and RPO requirements for systems.

Business Owners – Responsible for providing BIA information, working with Emergency Planning to provide RTO and RPO requirements, and participating in DR testing.

3. IT Disaster Recovery Policy

3.1 IT DR Management

3.1.1 ECC TS must develop, implement, maintain, and continually improve a set of documented processes which will support IT DR Management.

3.1.2 These processes must ensure that the IT DR objectives are clearly stated, understood, and communicated, and TS Senior Management's commitment to IT DR is demonstrated.

3.1.3 IT DR roles, responsibilities, competencies, and authorities must be defined and documented.

3.1.4 ECC TS Senior Management must ensure that all personnel who are assigned IT DR responsibilities are competent to perform the required tasks.

3.2 IT DR Requirements Analysis

3.2.1 ECC EP&R must provide Recovery Time Objective (RTO) and Recovery Point Objective (RPO) per ECC product, service, or activity.

3.2.2 ECC TS must document the achievable recovery time and recovery point for all critical IT services required to enable disaster recovery to take place.

3.2.3 Each critical IT service listed must identify the ECC product or service that it supports.

3.2.4 For each critical IT service identified all the IT components of the end-to-end service must be described and documented, showing how they are configured or linked to deliver each service.

3.2.5 A Service Owner for each critical IT service must be assigned and the details of this responsibility documented.

3.2.6 Standard appropriate maintenance contracts for critical IT components must be in place.

3.2.7 For each critical IT service the current IT DR arrangements must be compared with business continuity requirements, any gaps documented, and risk assessed, and reported to TS Senior Management.

3.2.8 TS Senior Management must sign off the IT service definitions, the documented list of critical IT services and the risks associated with gaps identified between critical IT DR capability and business continuity requirements.

3.2.9 Where critical services are outsourced, the Business Owner shall ensure that suppliers agree to have similar suitable plans and contingencies in place to meet the criteria for critical systems and applications and inform the TS Policy & Assurance team of all outsourced plans and contingencies.

3.3 IT DR Planning

3.3.1 ECC TS must have documented plans to manage potential disruption and enable continuity of IT services and the recovery of critical activities in the event of a disaster.

3.3.2 IT response plans and critical IT service recovery plans must be concise and accessible to those with responsibilities defined in the plans.

3.3.3 Contact lists for all TS staff required for disaster recovery must be maintained along with contact information for key ECC services (for example: DUCL, Buildings and Services (Mitie), Communications Team).

3.3.4 Critical IT service recovery plans must be documented such that competent personnel can use them in the event of an incident.

3.3.5 For each critical IT service the following information must be maintained:

1) Key system data: System owner, System Manager, platform details, backup mechanism, recovery mechanism, system tier ranking.
2) Key operational procedures for start-up, shutdown and recovery of all systems associated with the service.
3) Key contacts for suppliers, SLA details and maintenance contract details where relevant, and incident invocation and escalation procedures for the supplier. (As provided by the business owners)
4) Test schedule for system components, and full-service test schedule.

3.3.6 Operational procedures must be reviewed after significant or major changes to underlying systems and testing of services shall coincide with planned major upgrades.

3.3.7 ECC TS must document a clear process for standing down the IT DR Response Team once the incident is over and returning to business as usual.

3.3.8 Disaster recovery must be incorporated into the architecture of new systems that are deemed critical by the business.

3.4 IT DR Operations

3.4.1 ECC must use the incident management escalation and invocation protocols contained within the wider business continuity incident management plans to form the basis for managing potential IT related service disruptions.

3.4.2 The method by which an IT response and recovery plan is invoked must be clearly documented.

3.4.3 On invocation of a disaster the IT DR Response Team must be responsible for key decision making in relation to the management of the disaster.

3.4.4 All communications to and from teams outside of TS and related to the IT DR activities must be routed via the IT DR Response Team.

3.5 IT DR Testing and Plan Maintenance

3.5.1 Disaster recovery documents, specifically this policy, the recovery plans and procedures, must be tested and updated to ensure that they are up to date and effective, especially following significant system changes.

3.5.2 System level testing, including the physical hardware, must be tested on a regular basis to ensure that it operates as required and agreed with the Service Owner.

3.5.3 All testing must include a test plan in line with ECC Testing Policy.

3.5.4 Full results from all IT DR tests including proposed mitigating activities must be reported to the TS Leadership Team.

3.5.5 Regular reporting must be produced to inform TS Senior Management of the current state of DR management, DR test outcomes and upcoming DR tests.

4. Applicable Controls and References

- ISO 27301:2011 - Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
- ECC Information Security policies

5. Approval and updating

This policy was developed in conjunction with teams from Technology Services. It will be reviewed annually, and any proposed amendments will be submitted to the appropriate governance point for consideration and approval.

6. Exception to Policy

If you believe you have a valid business reason for an exception to any control statement specified in this policy, please raise a non-standard service request on ECC's Online Portal, clearly stating the following:

a. You require a TS Security Policy Exception – please state this at the start to allow easy identification of your request.
b. Which TS Security policy you need and exception against, and which controls statement(s) within it
c. Why you need the policy exception – State what will stop you adhering to the policy and please provide justification for not doing so.

Your requirement will then be investigated, any risk it causes assessed, and you will be advised of the outcome.

7. Document Control

Version	Date	Summary of Changes	Changes made by
1.00	August 2019	Approved and published.	TS Policy & Assurance
1.10	March 2021	Reviewed following Azure DR testing.	TS Policy & Assurance
1.11	June 2021	Minor formatting changes only	TS Policy & Assurance

Failure to comply with this policy and or other supporting policies or procedures may result in disciplinary action, dismissal or legal action being taken against you.