Essex County Council

Technology Services Security

Business Continuity Management Policy

Title	TS Security Business Continuity Management
Author / Owner	Technology Services Policy & Assurance
Intended audience	Technology Services employees, contractors, and any third parties working on its behalf.
Status	Live
Version	4.00
Last review	Oct 2022
Last approval	Oct 2022
Approved by	Head of Technology and Architecture
Next review	Oct 2023
Security Classification	Official

Contents

1. Purpose and Objectives

Essex County Council (ECC) manages a large amount of information to enable employees, third party contractors and anyone undertaking duties on behalf of the council to carry out their roles effectively and safely. The information is valuable and if appropriate technology security is not effectively implemented then harm and distress may be caused to the service users and individuals whose information we hold. Applicable legislation, company policies and standards also need to be adhered to.

In the case of a major event or disruption to council services, a business continuity plan is invoked to ensure critical services can continue to run. As well as providing business continuity and the availability of services, it is important that the plan includes the continuity of information security. This cannot cease in the event of a major event or disruption. Information must remain protected. This policy details the controls that need to be in place in the services Technology Services (TS) provides in order to ensure this.

This policy's objective is to ensure security continuity is embedded within TS business continuity.

2. Understanding the policy (Important: Please read first)

The controls in this policy are in addition to those specified by the Information Governance team (IG) in their Intranet based Information Governance Policy Booklet, and by TS in its Acceptable use of Technology Booklet (Currently in draft). All sets of controls are required to be adhered to.

Where the policy uses the terms 'services', 'systems', and 'users', it is referring to the services TS provides, the systems that form part of the services, and the users of the services.

2.1 Applicability

This policy applies to the services TS provides to its customers. Its controls are directed at all TS staff, contractors, and any third parties working on its behalf. The processes that this policy relates to are largely within TS. However, the services TS provides to users within other ECC functions and service areas will be delivered in line with this policy, and therefore subject to the principles herein.

2.2 External References and Guidance

Guidance from some external sources (standards etc.) assisted in the production of this policy, and it contains some references to them. An example of these are the reference numbers listed after each control statement, which refer to the related ISO/IEC 27001:2013 'Annex A' control number. The Applicable References section provides more details on this.

Security Policy guidance is available in the TS Security Policy Teams site. It explains why the policy controls/rules are required, and provides some high-level guidance on how they can be achieved.

2.3 Policy layout

This policy's requirements are spilt into sections and defined as control statements which when combined allow the objectives of the policy to be met.

3. TS Security Continuity (A.17.1)

3.1 Planning TS security continuity (A.17.1.1)

3.1.1 The requirements for TS security continuity and its management during disruptive events must be determined and documented within the TS business continuity management processes.

3.2 Implementing TS security continuity (A.17.1.2)

3.2.1 A business continuity management structure must be put in place to prepare for, mitigate, and respond to all disruptive events that could impact TS security continuity, utilising personnel with the necessary authority, experience, and competence.

3.2.2 Processes, procedures, and controls must be established, documented, implemented, communicated, and maintained to ensure the required level of TS security is maintained during disruptive events, and all those involved are fully aware of their roles and responsibilities.

3.2.3 Where it is believed that TS security controls will not be able to be maintained during disruptive events, compensating controls must be implemented to mitigate the risks, and ensure TS security continuity is maintained to an acceptable level.

3.2.4 Response and recovery plans for TS security services must link to the TS business continuity process and its plans.

3.3 Verify, review, and evaluate TS service security continuity (A.17.1.3)

3.3.1 Established and implemented TS security continuity controls must be verified at regular intervals (a minimum of annually) and upon significant system or process change in order to ensure they remain valid and effective during disruptive events.

3.3.2 Any business continuity planning exercises required by ECC's Emergency Planning team must be undertaken in order to ensure that relevant countermeasures against external and environmental threats are in place, remain effective, and maintain TS security continuity.

4. Applicable References

A list of the reference sources can be found below:

- ISO/IEC 27001:2013 - Information technology - Security techniques - Information Security Management Systems – Requirements:
  Annex 'A' reference numbers are specified at the end of control statements.
- Payment Card Industry (PCI) Data Security Standard Document Library:
  Requirement 12.10
- NHS Data Security and Protection Toolkit
  Data Security Standard 7- Continuity planning
- TS Security Policy 'Teams' site (contains TS Security Policy Guidance)
- Acceptable use of Technology Booklet (Currently in draft).

For further details on any of the above references, please contact: TS Policy & Assurance

The Information Governance Policy Booklet can be found on the ECC Intranet. If the link provided fails to work, type 'Information Policies' into ECC Intranet search facility, to locate it.

5. Approval and Updating

This policy will be reviewed annually, and any proposed amendments 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 do as follows:

a. Visit the TS Security Policy 'Teams' site.
b. Click on the button marked "Request a New Policy Exception"
c. Fill in the details requested in the form displayed and click on the 'Submit' button.

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

7. Stakeholder Signoff

Team	RACI	Signed off by	Date
Policy & Assurance	Responsible	Chris Hewitt	05/09/2022
Disaster Recovery Lead	Consulted	Rob Molnar	07/07/2022
Platform & Infrastructure	Consulted	Kevin Newton	19&31/05/2022
Applications - Core	Consulted	Louise John	19/04/2022
Application – Social Care	Consulted	David Woodward	09/06/2022
Service Ops – Service Desk	Informed	Kesiena Uzoh	Not required
Service Ops - Service fulfilment	Consulted	Shelley Edwards	16/05/2022
Service Ops – 2nd line and SME	Consulted	Shelley Edwards	17/06/2022
SSAM	Consulted	Kerry Duffy	16/06/2022
Enterprise Architect	Consulted	Philip Barbrook	30/05/2022
Security Architects	Consulted	Mike Kneller	26/04/2022
Service Architect	Consulted	Hayley Dack	17/05/2022
Business Engagement	Informed	Ron Isted	Not required
TS Training	Informed	Julie-Ann Newman	Not required
TS Testing	Consulted	Steve McGeary	14/06/2022
Servicer Operations Mgt	Consulted	Rhys Lovegrove	05/09/2022
Security Operations Centre	Consulted	Seyi Oni	14/09/2022

Evidence of each formal signoff must be retained. No signoff is needed where only 'Informed'.

8. Document Control

Version	Date	Summary of Changes	Changes made by
2.10	August 2017	Document reviewed; no changes made. The next review will follow the ISO 27001 status review.	IT Security
2.20	August 2019	Renamed and reviewed. Information specific controls updated.	TS Policy & Assurance
2.30	September 2019	Minor updates to links made.	TS Policy & Assurance
3.00	November 2020	Major review and update	TS Policy & Assurance
3.10	April 2021	Senior Manager Review	TS Policy & Assurance
3.20	May 2021	Approved for publishing	TS Policy & Assurance
3.30	Feb 2022	Stage 1 review conducted. Sent to stakeholder for review and signoff	TS Policy & Assurance
3.31	April 2022	Made available for Stage 2 Stakeholder review	TS Policy & Assurance
3.32	June 2022	Made available for Stage 3 Stakeholder review	TS Policy & Assurance
3.33	July 2022	Minor rewording performed resulting from stage 3 review feedback.	TS Policy & Assurance
3.34	Aug 2022	Additional signoff rows added (for new Joiners)	TS Policy & Assurance
3.35	Sep 2022	Stage 3 review signed off	TS Policy & Assurance
3.36	Sep 2022	Submission for stage 4 review	TS Policy & Assurance
4.00	Oct 2022	Stage 4 approval received. Due to the changes resulting from annual review, publishing as v4.00	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.