Category: ITS Policy Policy No.: ITS-04-2024 Revisions: February 7, 2024	middlesex centre in the centre of it all	Pages: 6 Effective Date: February 7, 2024 Report No.: CPS-06-2024

Information System Disaster Recovery and Business Continuity Policy

Purpose

The purpose of this policy is to establish processes to ensure the availability of all information systems required for essential business operations in the event of an equipment failure, service disruption, or a loss of operational capacity resulting from a fire, natural disaster, or other emergency.

This policy addresses business continuity for information systems and recovery of information systems.

Scope

This policy applies to Members of Council, all employees of Middlesex Centre including Paid-on-Call Firefighters and volunteers. It applies to all IT assets of the municipality.

Definitions

For the purpose of this document, the following terms have the following meanings:

"Business mission-critical system" is defined as an information system that is required to support essential business functions during both normal operations and during a disaster or other event that may limit the municipality's capacity to conduct normal operations. Some business functions may not be mission-critical if loss of these system functionality does not adversely affect the municipality's ability to conduct essential business operations.

"Departments" means any categorical division of service delivery or municipal administration of Middlesex Centre which is officially recognized by Middlesex Centre and exercises powers delegated to it by Middlesex Centre, including but not limited to any local board (as defined by the Municipal Act, 2001 as amended or replaced) that exercises powers delegated to it by Middlesex Centre.

"External services" are defined as services that are provided by an external provider, such as a power company or Internet Service Provider (ISP).

"Information system" is defined as a system that is required to process information used in business operations. An information system includes all of the hardware, operating system

software, application software, network connections, and external services required for proper operation.

"ITS" means Information Technology Services.

"Maximum Tolerable Downtime (MTD)" is defined as the maximum amount of time that an information system can remain non-functional before business operations are adversely affected.

"Middlesex County ITS" is the department at Middlesex County responsible for procurement, maintenance, and support of Information Systems on behalf of Middlesex Centre.

"Off-site location" is defined as a physical location that is geographically distant from municipal offices and/or facilities such that no single weather-related or other disaster would be likely to affect both locations.

"Public or private cloud" is defined as a collection of hardware and software that is located in a secure location with redundant systems for power and internet connectivity. Public clouds are multi-tenant data centres where computing infrastructure can be purchased at a required capacity on either a temporary or permanent basis. Private clouds are owned by the municipality or an affiliate and are not available to the general public.

"Recovery Initiation Point (RIP)" is the time when recovery should be initiated. This typically occurs when the time since system failure plus the Recovery Time Objective is equal to the Maximum Tolerable Downtime. For example, if the RTO is 1 hour and the MTD is 5 hours, recovery should be initiated 4 hours after system failure. RIP can also be expressed as MTD minus RTO.

"Restore Point Objective (RPO)" is defined as the maximum amount of data loss that can be tolerated in terms of time. If the RPO is 1 hour, then restore points must be created on an hourly basis.

"Restore Service Level (RSL)" is defined as the required capacity of an information system for minimal or interim operations. If a system operating at 50% of its normal operating capacity is adequate to support minimal business operations during a failure or disaster event, then the RSL is 50%.

"Restore Time Objective (RTO)" is defined as the time required to restore an information system from its maintained (back-up) state to the Restore Service Level, establish connectivity, and make it available for business operations.

Responsibilities

Middlesex County's Information Technology Director, as per their contracted role with the Municipality of Middlesex Centre, shall be appointed the municipality's IT Security Officer. The IT Security Officer, in conjunction with the municipality, shall be responsible for ensuring implementation of all items listed in the policy requirements section which follows.

Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Middlesex Centre's employees are responsible for following the guidelines provided and using the information systems correctly and in compliance with municipal policies and procedures on information technology.

Policy Requirements

This policy works in conjunction with Middlesex Centre's Information Security Disaster Recovery and Business Continuity Plan.

Middlesex Centre's IT Security Officer in conjunction with the municipality shall ensure compliance with the following standards:

a) The Municipality shall create and maintain the Information Security Disaster Recovery and Business Continuity Plan. This plan shall be tested by the IT Security Officer to ensure proper back-up and recovery of critical business data.

b) A Recovery Time Objective (RTO) must be determined for critical systems. System dependencies must also be determined and considered. The RTOs must always be less than the Maximum Tolerable Downtime (MTD). System RTOs must be documented and logged to inform future Business Continuity Plan tests. System RTOs are documented in the Information Systems Disaster Recovery and Business Continuity Plan, which shall be updated and reviewed annually.

c) All servers and data storage devices must be protected by Uninterruptable Power Supply (UPS) devices to protect against power fluctuations and short-term disruptions.

d) Hardware should be identified and documented in an asset register. This should include all local network hardware, remote location hardware, remote location with company owned hardware (co-location), and public or private cloud storage locations on which system recovery will run.

e) Where possible, external services should be redundant (e.g., multiple ISP connections, on-site power generators, etc.).

f) Testing of the Information Systems Disaster Recovery and Business Continuity Plan should occur annually. The test should be fully documented in a post-test report, and future tests demonstrably informed by the previous test's activities. Refer to Appendix B for testing log.

Communication of the Policy

The CAO will work with the IT Security Officer who shall communicate this policy to appropriate individuals as necessary to ensure proper implementation.

All Middlesex Centre employees with roles in purchasing, installing/implementing and/or maintaining information systems infrastructure shall review and acknowledge this policy.

Compliance

Corporate Services and Middlesex County ITS enforce this policy and related standards. Anyone who has reason to suspect a deliberate and/or significant violation of this policy is encouraged to promptly report it to the Middlesex County ITS Service Desk. Policy violations that come to the attention of the ITS Service Desk will be escalated to the Director of ITS and Director of Corporate Services.

Staff in violation of this policy may be subject to disciplinary action up to and including termination.

Policy Review

This policy will be reviewed once every four (4) years, or as necessary.

Appendix A: Acknowledgement of Policy – Contracted Service

I have reviewed this policy and have had an opportunity to ask any questions regarding the requirements. If I have further questions, I will bring them to the attention of my supervisor.

The Municipality of Middlesex Centre takes the above-policy, the Municipal Act and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) requirements with utmost seriousness. For those that do not strictly comply with them:

- Middlesex Centre Employees – may face discipline up to and including employment termination.
- Employees of Contracted Services – may face formal complaints to the IT Security Officer. If the matter is not rectified, legal steps may be taken to address the concern.

Employee Name (print): _____

Employee Position: _____

Employee Department: _____

Employee Signature: _____

Date: _____

Appendix B: Policy Testing Log

Date Testing Occurred	Results	Signature of IT Security Officer