

If you have questions or comments, please contact:

Tony Campbell

Enterprise IT Security Specialist

tcampbell@rochestermn.gov

(507) 328-2848

Section 9: IT BUSINESS CONTINUITY

The objective of Information Technology (IT) Business Continuity Management is to ensure the continued operation and secure provision of essential services during a disruption of normal operating conditions. The purpose of this section is to define IT business continuity preparedness, response, and recovery capabilities.

Goals of Section 9: IT Business Continuity

- Demonstrate the City's commitment to IT business continuity.
- Require and assign responsibility for an annual business impact assessment (BIA).
- Require the City to have an IT Business Continuity Plan and assign management responsibilities for IT business continuity.
- Ensure that the City is prepared to respond to, and recover from, disruptions to IT systems.
- Ensure that the City can continue to provide essential services during the recovery period.

IT business continuity Policy Index

9.1. Business Impact Analysis (BIA)

9.2. IT Business Continuity Plan

9.3. IT Business Continuity Management

9.4. IT Disaster Recovery Plan

9.5. IT Continuity Testing and Maintenance

9.1. Business Impact Analysis (BIA)

9.1.1. The Technology Steering Committee is responsible for scheduling an enterprise-wide annual BIA. System owner participation is required.

9.1.2. The BIA will identify essential (critical) IT services and processes. Essential requires meeting one or more of the following criteria:

9.1.2.1. Law, regulation, or contractual obligation makes the service a requirement.

9.1.2.2. Disruption would be a threat to public safety.

9.1.2.3. Disruption would affect the health and well-being of employees.

9.1.2.4. Disruption would result in irreparable harm to customers or business partners.

9.1.2.5. Disruption would result in significant or unrecoverable financial loss.

9.1.3. For each essential service and/or process, the maximum tolerable downtime (MTD) requires documentation. The MTD is the total length of time an essential function or process can be unavailable without causing significant harm to the City.

9.1.4. For each essential service and/or process, supporting infrastructure, devices/information systems and dependencies require identification.

9.1.5. A recovery time objective (RTO) and recovery point objective (RPO) will be identified for each essential service or process. 9.1.6. Current RTO's and RPO's versus desired capability for essential services and processes will be identified. Deviations require reporting to the Technology Steering Committee.

9.1.7. The Technology Steering Committee and the IT Leadership Team are jointly responsible for aligning the BIA outcome with the IT Business Continuity Plan.

9.2. IT Business Continuity Plan

9.2.1. The City's IT business continuity strategy requires documentation in a IT Business Continuity Plan that supports the Cities Continuation of Operations (COOP). The plan shall include plans, procedures, and ancillary documentation related to, contingency operations, recovery, resumption, training, testing, and plan maintenance.

9.3. IT Business Continuity Management

9.3.1. Department Heads or their appointed agents are responsible for authorizing the IT Business Continuity Plan. The IT Business Continuity Plan is inclusive of IT plans, procedures, and ancillary documentation related to IT contingency operations, recovery, resumption, training, testing, and plan maintenance.

9.3.1.1. IT Leadership Team will report on the status and test results of the IT business continuity plan at least annually and inform the Technology Steering Committee on a timely basis of any material changes to the IT business continuity strategy.

9.3.2. The IT Leadership Team is responsible for the development, maintenance, and management of the IT business continuity strategy and plan.

9.3.3. The City Technology and Finance Director, with the support of the Department Heads will include IT business continuity expenses in the annual operating budget.

9.3.4. The IT Leadership Team is responsible for designing, testing and supporting resilient systems that meet the RTO and RPO for the recovery of information and information systems in a disaster situation.

9.3.5. Department Heads are responsible for defining and prioritizing the essential IT systems needed to support their departments and for creating and maintaining functional departmental contingency procedures in the event of the loss of an essential IT system.

9.4. Disaster Recovery Plan

9.4.1. The IT Leadership Team is responsible for the IT Disaster Recovery Plan. The IT Disaster Recovery Plan is a component of the Cities COOP.

9.4.2. The IT Disaster Recovery Plan must include recovery strategies and procedures for systems and facilities as determined by the BIA.

9.4.3. The Technology Steering Committee must approve modifications to the recovery plan.

9.4.4. The amount of procedural detail required should be enough that competent personnel familiar with the environment could perform the recovery operation.

9.4.5. The recovery plan must reflect any external system dependencies and relevant contractual agreements.

9.4.6. Personnel responsible for recovery operations must receive appropriate training.

9.4.7. IT Recovery plans and procedures require testing in accordance with the schedule set forth as part of the BIA.

9.4.8. The IT Leadership Team will report at least annually on the status and testing results of the IT Business Continuity Plan to the Technology Steering Committee

9.5. Continuity Testing and Maintenance

9.5.1. Reference to the IT Business Continuity Plan is inclusive of plans, procedures, and ancillary documentation related to IT disaster preparation, response, contingency operations, recovery, resumption, training, testing, and plan maintenance.

9.5.2. The IT Leadership Team is responsible for maintenance of the IT Business Continuity Plan.

9.5.3. The Technology Steering Committee will conduct an annual review of the IT Business Continuity Plan.

