Municipal Technical Advisory Service
INSTITUTE FOR PUBLIC SERVICE

Published on *MTAS* (https://www.mtas.tennessee.edu) September 17, 2019

Developing an IT Disaster Recovery Plan

Dear Reader:

The following document was created from the MTAS website (mtas.tennessee.edu). This website is maintained daily by MTAS staff and seeks to represent the most current information regarding issues relative to Tennessee municipal government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with municipal government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other MTAS website material.

Sincerely,

The University of Tennessee
Municipal Technical Advisory Service
1610 University Avenue
Knoxville, TN 37921-6741
865-974-0411 phone
865-974-0423 fax
www.mtas.tennessee.edu

Table of Contents

Developing an IT Disaster Recovery Plan

Reference Number: MTAS-2116

A disaster recovery plan (DRP) should be a collaborative process. At the minimum, you will need to have a knowledgeable representative from each department or area of the city that is touched by Information Technology. By involving as many of your users as possible, you will increase your ability to capture all the necessary information. Each representative will provide you with information about the types of services, software, and hardware that they would need in order to perform their respective jobs.

Step One

Your starting point for DRP should be a comprehensive inventory of hardware (servers, desktops, laptops, printers, wireless devices, routers, switches, etc.), software applications, and data. Your goal is to account for everything you would need to do business in the event of any or all types of disasters. Consider and document the different types of disasters that you are planning for and include disasters that your area or location might be more prone to for the specific location. For example, city hall is located in a flood zone. Include everything you would need to work at city hall or your disaster recovery site with redundancy, if physically and financially feasible (power, data connectivity, equipment, etc.).

Step Two

As part of the inventory, or once it is complete, take the time to classify or understand the impact level of your data and/or the security classification of the data. This information will be useful in the development of an IT Security Plan, a Business Continuity Plan, as well as with the DRP. Also make note of where the data is located (server drive or local PC). The Federal Information Processing Standard 199 (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems (2004) [1] defines three security objectives for information and information systems:

- Confidentiality – A loss of confidentiality is the unauthorized disclosure of information.
- Integrity – A loss of integrity is the unauthorized modification or destruction of information.
- Availability – A loss of availability is the disruption of access to or use of information or an information system.

Each of these is evaluated for the level of potential impact on the organization or individuals should there be a breach of security, loss of access, or in this case, a disaster of some sort.

- Low – The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
- Moderate - The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
- High - The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

While the availability is the most important security objective for developing your DRP, you need to keep all three objectives in mind during the planning process, as well as during a recovery process, to avoid breaching or compromising either of the other two during a recovery or disaster scenario.

Step Three

Once you have completed the inventory, including security classifications, you are ready to create the DRP. Begin developing the DRP based on the services you need to provide immediately following a disaster. Classify your hardware based on the same structure outlined above, as this will help you triage your equipment, in the event of a disaster. The DRP will help you reassign equipment from less critical services to more critical applications in order to get them up and running sooner, or until you are able to replace affected hardware. Classifying your hardware and equipment will be especially helpful if you plan to use existing low-use or low-priority equipment as your DRP replacements.

Step Four

Once you have a final DRP in place, you will want to test the DRP. Use the testing process to evaluate and further tune your DRP. You will want to update or evaluate the DRP annually to make sure that it stays current. Also, make sure to revisit the DRP as your environment changes.

Helpful Links

U [2]T Emergency Management Policy [3]

UT IT0128 - Contingency Planning [4]

Metro Government Nashville IT Contingency/Disaster Recovery Planning [5]

N [6]IST Computer Security Resource Center - Disaster Recovery Documents Search [7]

NIST CSRC SP 800-60 Vol. 1 Rev. 1 [8]

NIST CSRC SP 800-60 Vol. 2 Rev. 1 [9]

N [1]IST FIPS PUB 199 [10]

Links:
[1] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
[2] https://universitytennessee.policytech.com/dotNet/documents/download.aspx?docid=158&amp;DocRevisionNum=1&amp;SaveToMyComputer=true&amp;rnd=1513035234851&a
[3] https://universitytennessee.policytech.com/docview/?docid=178&amp;public=true
[4] https://universitytennessee.policytech.com/docview/?docid=167&amp;public=true
[5] https://www.nashville.gov/Portals/0/SiteContent/ITS/docs/Information%20Security/14_ITContingencyDisasterRecoveryPolicy.pdf
[6] http://csrc.nist.gov/publications/PubsSPs.html
[7] https://csrc.nist.gov/publications/search?keywords-lg=disaster+recovery&amp;sortBy-lg=Number+DESC&amp;viewMode-lg=brief&amp;ipp-lg=ALL&a
[8] https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final
[9] https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final
[10] https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

DISCLAIMER: The letters and publications written by the MTAS consultants were written based upon the law at the time and/or a specific sets of facts. The laws referenced in the letters and publications may have changed and/or the technical advice provided may not be applicable to your city or circumstances. Always consult with your city attorney or an MTAS consultant before taking any action based on information contained in this website.

Source URL (retrieved on *09/17/2019 - 9:08pm*): https://www.mtas.tennessee.edu/reference/developing-it-disaster-recovery-plan

Municipal Technical Advisory Service
INSTITUTE FOR PUBLIC SERVICE