Disaster Recovery Policy

Purpose

The purpose of the (District/Organization) Business Continuity and Disaster Recovery Policy is to provide direction and general rules for the creation, implementation, and management of the (District/Organization) Disaster Recovery Plan (DRP).

Audience

The (District/Organization) Disaster Recovery Policy applies to individuals accountable for ensuring a disaster recovery plan is developed, tested, and maintained.

Policy

* (District/Organization) must create and implement a Business Continuity and Disaster Recovery Plan (“BDRP”).
* The DRP must be periodically tested and the results should be used as part of the ongoing improvement of the DRP.
* The DRP, at a minimum, will identify and protect against risks to critical systems and sensitive information in the event of a disaster.
* The DRP shall provide for contingencies to restore information and systems if a disaster occurs. The concept of a disaster recovery includes business resumption.
* (District/Organization) disaster recovery planning must ensure that:
  + an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
  + personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security are nominated;
  + documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.
* The (District/Organization) DRP must include at a minimum, the following elements:
  + Business impact analysis, including risk assessment, Information Resource asset classification, and potential disruption to stakeholders
  + A classification system to identify critical systems and essential records
  + Mitigation strategies and safeguards to avoid disasters. Safeguards should include protective measures such as redundancy, fire suppression, uninterruptible power supply (UPS), surge protection, and environmental measures to protect sensitive equipment from dust, temperature, or humidity
  + Backups and offsite storage
  + Information Resource role in business resumption
  + Contingency plans for different types of disruptions to Information Resource and systems availability
  + Organizational responsibilities for implementing the disaster recovery plan
  + Procedures for reporting incidents, implementing the disaster recovery plan, and escalating (District/Organization)'s response to a disaster
  + Multiple site storage of back-up documents
  + Training, testing, and improvement
  + Annual review and revision

Definitions

See Appendix A: Definitions

References

* ISO 27002: 17
* NIST CSF: ID.BE, PR.IP, RS.RP, RS.CO, RS.IM, RS.RP, RC.IM, RC.CO
* (District/Organization) Information Classification and Handling Policy

Waivers

Waivers from certain policy provisions may be sought following the (District/Organization) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Modified Date | Approved Date | Approved By | Reason/Comments |
| 1.0.0 | February 2018 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |