Incident Management Policy

Purpose

The purpose of the **(District/Organization)** Incident Management Policy is to describe the requirements for dealing with security incidents.

Audience

The (District/Organization) Incident Management Policy applies to individuals that use any (District/Organization) **Information Resource**.

Contents

[Incident Reporting](#_Incident_Reporting)

[Response Team](#_Response_Team)

Policy

### Incident Reporting

* Personnel are required to promptly report possible or known information security and confidentiality violations to (District/Organization) IT; including the following:
	+ Infrastructure incident: any event considered to be a malicious action that causes a failure, interruption, or loss in availability to any (District/Organization) **Information Resource**.
	+ Data incident: any loss, theft, or compromise of (District/Organization) information.
	+ Unauthorized access incident: any unauthorized access to a (District/Organization) **Information Resource**.
* Potential incidents and threats reported from event logging, vulnerability management, and other monitoring activities must be reported to (District/Organization) IT.
* All reported incidents must be assessed by (District/Organization) IT to determine the threat type and activate the appropriate response procedures.

### Response Team

* Incident Response Commander will establish and provide overall direction to an (District/Organization) Incident Response Team (IRT).
* The Incident Response Commander is responsible for overseeing the creation, implementation, and maintenance of an Incident Management Plan.
* (District/Organization) IRT members have pre-defined roles and responsibilities which can take priority over normal duties. Any additional (District/Organization) staff member may be called upon to assist in resolving an incident.
* The IRT will respond to any new threat to (District/Organization) information systems or data following the Incident Management Plan.
* The Incident Response Commander must report the incident to:
	+ (District/Organization) Executive Management
	+ Any affected customers and or/partners
	+ Local, state, or federal law officials as required by applicable statutes and/or regulations.
* The Incident Response Commander or executive management team will coordinate communications with any outside organizations.
* The Incident Management Plan must be tested by the IRT no less than annually.
* The IRT must participate in training activities specific to the organization’s Incident Response Plan at least annually or upon significant change to the organization.

Definitions

See Appendix A: Definitions

References

* ISO 27002: 16
* NIST CSF: PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS-IM, RC.CO

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 | October 2019 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |