Policy Title Security Incident Management Policy
Department Information Services
Chapter 5
Section 9
Policy 2
Effective Date Friday, April 2, 2021

POLICY STATEMENT

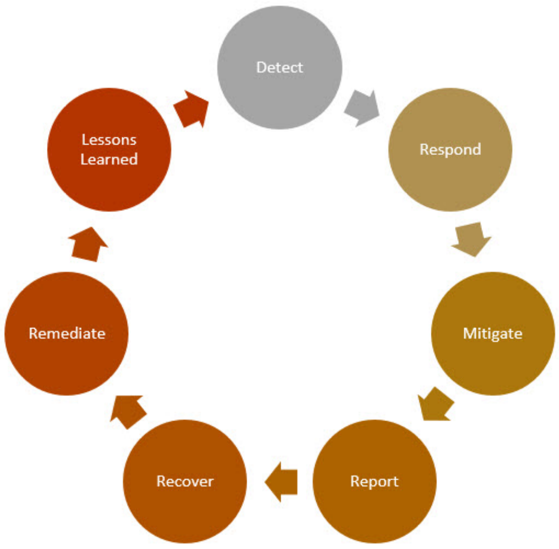
Ramsey County is committed to managing security incidents to limit their damage, while ensuring that the appropriate individuals and agencies are notified in accordance with law.

APPLICABILITY

This policy applies to all incidents concerning assets and information managed by Ramsey County, on premise and off premise. This policy addresses the requirements outlined in HIPAA §164.308(a)(6) and CJIS section 5.3 (Incident Response) and section 13.5 (Mobile Device Incident Response).

GENERAL INFORMATION

Security incidents may be accidental or intentional and may result in unauthorized disclosure of information, loss of information integrity, or loss of service availability. Security incident management follows seven steps as indicated below.



- **Detection:** Ramsey County will implement systems and processes to detect potential security incidents.
- **Response:** A security response team will be identified to investigate potential security incidents as they occur.
- **Mitigation:** Mitigation attempts to limit the effect or scope of an incident by preventing further damage while still allowing for data forensics to aid in root cause analysis.
- **Reporting:** Security breaches will be reported as required by county policy and law.
- **Recovery:** Affected systems will be replaced, rebuilt, or otherwise returned to operational status when it is safe to do so.
- **Remediation:** The IS team or their designated agents will look at the incident and attempt to identify what allowed it to occur and implement methods to prevent it from happening again.
- **Lessons Learned:** This final step will examine the incident and the response to see if there are any lessons to be learned.

AUTHORITY

This policy and the procedures herein were prepared under the authority of the County Manager, as delegated to the Ramsey County Chief Information Officer.

DEFINITIONS

The following definitions are in the **Information Services Data Dictionary**:

- **Security Incident**: A security incident is any event that threatens the confidentiality, integrity, or availability of Ramsey County information assets, information systems, or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident. Incidents may include but are not limited to unauthorized entry, security breach or potential security breach, unauthorized scan or probe, denial of service, malicious code or virus, violations of Ramsey County security policies, and system outages.
- **Security Breach:** A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.

RESPONSIBILITIES

Ramsey County

- Ensure the confidentiality, integrity, and availability of its data and customer data stored on its systems.
- Relevant executives will be aware of any major security incidents and will be responsible for managing all appropriate and lawful communication pertaining to those incidents.

Departments

- Departmental managers will participate in handling security incidents where necessary. This will include security incidents that affect their staff, their processes, or the systems that their department manages.

Information Services Security

- Information Services Security will log a ticket and will categorize that ticket as a security incident. If known, I.S. Security will identify the incident as intentional or accidental and will identify those involved.
- Information Services Security will update this policy to stay relevant with security challenges and organizational structure. This includes updates to the policy that may be identified in Lessons Learned.
- Information Services Security will oversee all incident management processes contained within this policy, which includes securing evidence and maintaining its integrity.
- Information Services Security will socialize this policy with departmental managers and appropriate individuals to ensure understanding.
- Information Services Security will own the incident management standard that conforms with this policy.

Designated support teams (Information Services and business)

Ramsey County has a distributed technology infrastructure support model. The following groups are responsible for managing system configurations in their designated domain of responsibility.

1. IS Infrastructure system administrators manage most of the Microsoft Windows Server, MS database, and MS backup office technologies.
2. IS infrastructure network administrators manage most of the Cisco network solutions.
3. IS desktop support technicians manage most of the desktop and peripheral devices.
4. Sheriff's Office, Office of Information & Technology, manages a variety of technologies server, desktop, peripherals, and networks.
5. Library Services, Office of Information & Technology, manages a variety of technologies, including servers, desktops, peripherals, and networks.
6. Application support and capability teams manage applications and business services.
7. Vendors manage a variety of 3rd party-supported technologies, including servers, desktops, peripherals, and networks.

Each of the above-reference support teams will:

- Report potential security incidents to Information Services, relevant departments, and other agencies as required by law.
- Preserve all logs, evidence, and other information that may be used to investigate the security incident, even after the incident has been contained.
- Assist Information Security, other departments, and agencies during an incident investigation that affects the services and devices within their departments.

Users

- All employees are part of the first stage of incident management, which is detection. Employees will remain vigilant to any potential security incidents and will report them Information Services Security.
- Complete the mandatory annual Ramsey County information security training.

LINKS AND RESOURCES

- **Security Incident Management Standard**
- Incident Management Policy

CONTACTS / SUBJECT MATTER EXPERTS

- Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
Dec. 14, 2020	Initial Draft

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, February 2021
Revision History Date Monday, April 5, 2021

Security Incident Response Standard

‹ Major Incident (Priority 1) **Back** **Security Incident Response Standard ›**