# One-Page Emergency Incident Response Plan

# Security Incident Management RACI Chart

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roles | R = Responsible  A = Accountable  C = Consulted  I = Informed | Help Desk | Cybersecurity | IT Operations | CISO | Legal | HR | Public Relations | Senior Management |  |  |  |
| Determine the scope and impact of the incident | |  |  |  |  |  |  |  |  |  |  |  |
| Communicate with senior management about significant incidents | |  |  |  |  |  |  |  |  |  |  |  |
| Determine if any regulatory, legal, or compliance mandates have been impacted, including breach notification requirements. | |  |  |  |  |  |  |  |  |  |  |  |
| Isolate or disconnect any infected endpoints or servers from the network, if necessary. | |  |  |  |  |  |  |  |  |  |  |  |
| Disable compromised user accounts, change passwords, or remove privileges, if necessary. | |  |  |  |  |  |  |  |  |  |  |  |
| Implement public relations / communications campaign to reduce reputational damage as appropriate. | |  |  |  |  |  |  |  |  |  |  |  |
| Eliminate the root cause of the incident (e.g. remove malware, block unauthorized users). | |  |  |  |  |  |  |  |  |  |  |  |
| Restore data from backups. | |  |  |  |  |  |  |  |  |  |  |  |
| Restore servers and other systems, as necessary. | |  |  |  |  |  |  |  |  |  |  |  |
| Perform vulnerability assessments, anti-malware scans, and other tests to verify that operations are back to normal. | |  |  |  |  |  |  |  |  |  |  |  |
| Communicate with stakeholders that the incident is resolved, next steps, etc. | |  |  |  |  |  |  |  |  |  |  |  |
| Facilitate post-incident lessons learned meetings, when appropriate. | |  |  |  |  |  |  |  |  |  |  |  |

**Threat Escalation Protocol**

A TEP outlines the escalation procedures for incidents, and the type of stakeholders needed during the incident management process. Identify the threat escalation protocol for your organization based on the impact and scope of criteria of your organization. Refer to the TEP participant table to better understand which stakeholders are involved in the different level TEP tier levels. Also refer to the scope and impact criteria tables on the slide for further details on the criteria levels.

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Escalation Protocol (TEP)** | | | |
| **Impact** | **Scope** | | |
| **High** | **Medium** | **Low** |
| **High** |  |  |  |
| **Medium** |  |  |  |
| **Low** |  |  |  |

|  |  |
| --- | --- |
| Threat Escalation Protocol (TEP) | Participants |
| TEP Tier 1 | End User, Help Desk, Cybersecurity, IT Operations, CISO, Legal, HR, PR, Senior Management, External Third Parties |
| TEP Tier 2 | End User, Help Desk, Cybersecurity, IT Operations, CISO |
| TEP Tier 3 | End User, Help Desk, Cybersecurity |

# Data Breach Regulator

|  |  |
| --- | --- |
| Regulators | |
|  |  |
|  |  |

# Communication Checklist

When communicating an incident, ensure enough context and essential information is provided. Consider the following:

* Summary of incident.
* What assets (data/devices) were affected?
* Who was affected (e.g. internal staff, clients/customers, business partners, suppliers)?
* What are the risks of the data being exposed?
* How will updates be communicated?
* Which external parties need to be notified (e.g. customers, regulators, law enforcement, insurance)?
* What is being done to contaminate and mitigate the incident?
* What should end users do now?
* What services are being offered to those affected? Who to contact for assistance or more information?
* Do I need to start the process of data recovery and/or DRP?
* What are lessons learned?

**Info-Tech Material**

1. **Security Incident Management RACI Chart**

[Develop and Implement a Security Incident Management Program](https://www.infotech.com/research/ss/develop-and-implement-a-security-incident-management-program) (Blueprint)

* Security Incident Management RACI Tool (Excel Tool)

1. **Threat Escalation Protocol**

[Develop and Implement a Security Incident Management Program](https://www.infotech.com/research/ss/develop-and-implement-a-security-incident-management-program) (Blueprint)

* Security Incident Management Plan (Word Document)

1. **Data Breach Requirements**

[Mature Your Privacy Operations](https://www.infotech.com/research/ss/mature-your-privacy-operations) (Blueprint)

Data Breach Reporting Requirements Summary (Word Document)

1. **Communication Checklist**

[Master Your Security Incident Response Communications Program](https://www.infotech.com/research/ss/master-your-security-incident-response-communications-program) (Blueprint)

Security Incident Communications Guidelines and Templates (Document)