Privileged Account

Incident Response Plan Template

**ABOUT THIS TEMPLATE**

This template is a customizable checklist to help you respond to a cyber attack, based on security industry best practices and hands-on experience protecting sensitive information and systems for companies of all sizes. It is designed to set the foundation for an incident response strategy that is proactive, pragmatic, and simple to adopt.

Action steps included in the incident response template focus on the importance of protecting privileged accounts to prevent a cyber attack from escalating. When privileged accounts are compromised, the potential impact of a breach increases as does the time it takes to identify and eliminate the attacker. We've prioritized actions that help you discover and shut down an attack quickly and effectively while maintaining business continuity.

You can customize this template to define your risk criteria, roles and responsibilities, and crisis communication strategies. This is a key resource to coordinate the efforts of everyone in your organization involved in incident response – security leaders, operations managers, help desk teams, identity, and access managers, as well as audit, compliance, communications, and executives.

In addition to this customizable template, incident response toolkit includes the whitepaper, [How to Protect Privileged Accounts with an Incident Response Plan](http://thycotic.com/resources/cyber-incident-response-plan/) outlines proactive steps you can take to protect your most vulnerable assets and lower your risk of a catastrophic cyber attack.

### 

### Customizing the Template

To customize this, perform the following steps:

1. Download the template.
2. Open the template as a Microsoft Word document.
3. Remove the About this Template and Customizing the Template instructions.
4. Replace the term Company X with the name of your organization.
5. Replace the current logo with your company logo.
6. Follow the instructions located in italics throughout this template, then delete the italic instruction sections.
7. Update all company-specific contact information.
8. Update the document identification details.
9. Revise to meet your needs.
10. Save your changes.
11. Share and gather feedback from everyone involved in your incident response team. Make sure everyone understands their role and the compliance and legal requirements your company must consider during an incident.
12. Distribute the plan according to your management guidance.

### 

### Disclaimer

This document is a template only and should be revised to meet the information security guidelines of your organization. Organizations should not adopt any security policy or plan without proper review and approval by senior management, information security, and legal.

# 

# **Ownership and Approval**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Policy Owner and Title | Phone | Email | Date | Signature |
| Contact |  |  |  |  |
| Approved By |  |  | Date | Signature |
| Executive Sponsor |  |  |  |  |

# **Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Description | Policy # | Revision Date | Review  Date | Reviewer/  Approver Name |
| 1.0 | Initial Version |  |  |  |  |
|  |  |  |  |  |  |

# **Compliance Requirements**

*Include a list of compliance requirements that impact your organization as a quick reference here. For a list of compliance mandates that may impact you, see Appendix A.*

|  |  |
| --- | --- |
| Compliance Rule | Description |
|  |  |
|  |  |

**EXECUTIVE SUMMARY**

To maintain the trust of our employees, customers, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyber attack. The more we are prepared to respond to a potential cyber attack, the faster we can eradicate any threat and reduce the impact on our business.

The goal of this incident response plan is to prepare *[company name]* to quickly and effectively contain a cyber threat while we continue our normal business operations. To this effect, actions outlined in the plan pay special attention to protecting privileged accounts that provide access to critical systems such as databases, applications, and networks. These include service, application and root accounts, network and administrator accounts, and local domain accounts.

Effective incident response involves every part of our organization, including IT teams, legal, technical support, human resources, corporate communications, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be updated *[at least annually]* to reflect our changing organization, new technologies, and new compliance requirements that inform our cyber security strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

**IMMEDIATE MITIGATION ACTIONS**

Regardless of how we may have discovered a security incident or breach, there are several tasks that our IT security team needs to consider taking immediately.

* Disable existing Domain Administrator accounts and move to new accounts
* Rotate all local and domain credentials
* Lock down the OS environment and carefully update it with any security patches relevant to the breach
* Discover newly created accounts as of the incident/breach date and audit activity
* Audit and monitor privileged accounts for suspicious activity
* Reset Kerberos Tickets

**ROLES, RESPONSIBILITIES & CONTACT INFORMATION**

*To properly respond to a cyber incident, it is important to consider all ways it can impact the company. This means including a cross-functional team of people who can manage the systems, legal, and communication issues that arise.*

*Below is a list of roles within an organization required to conduct a comprehensive, coordinated incident response. You can customize this list to match the size, structure, and regulatory and industry requirements of your organization. For example, one person may fill several roles or several people may coordinate to share the responsibility of a single role. Security tools may support the efforts of people involved in the incident response team, but they do not replace them; each tool must have an owner who is ultimately responsible for using it to fulfill the responsibilities of the role they are assigned.*

*Include contact information for everyone involved in incident response, both internally and externally. Note that a cyber attack could render critical systems like email or VoIP unavailable. Therefore, it is a good idea to plan for alternative communications systems and back-up contact information. You should also keep a hard-copy of your incident response plan and contact information accessible.*

|  |  |  |
| --- | --- | --- |
| Role | Responsibility | Contact Details |
| **INFORMATION SECURITY** | | |
| Chief Security Officer  OR  Chief Information Security Officer | Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan.  Authorizes when and how incident details are reported.  Main point of contact for executive team and Board of Directors. | Name  Phone  Email |
| Incident Response Team Lead and Team Members | Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident.  Maintains incident response plan, documentation, and catalog of incidents.  Responsible for identifying, confirming and evaluating extent of incidents.  Conducts random security checks to ensure readiness to respond to a cyber attack. | Name  Phone  Email |
| Identity and Access Team Lead and Team Members | Responsible for privilege management, enterprise password protection and role-based access control.  Discovers, audits, and reports on all privilege usage.  Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are.  Monitors privileged account uses and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior.  Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks.  Takes action to prevent the spread of a breach by updating privileges. | Name  Phone  Email |
| IT Operations and Support (internal) | Manages access to systems and applications for internal staff and partners.  Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyber attack. | Name  Phone  Email |
| Technical Partners (Internet Service Provider, Managed Service Providers, Hosting, Testing Partners, etc.)  Third Party External Incident Response Teams | Manages security controls to limit the progression of a cyber attack across third-party systems and organizations.  Coordinates with Internal Response Team to manage risks. Professional Incident response teams help ensure a solid Incident Response process is followed. It is always good to have an external expert incident response team available who have some existing knowledge of your environment. | Name  Phone  Email  Name  Phone  Email |
| **COMPLIANCE** | | |
| Legal Counsel | Confirms requirements for informing employees, customers, and the public about cyber breaches.  Responsible for checking in with local law enforcement.  Ensures IT team has legal authority for privilege account monitoring. | Name  Phone  Email |
| Audit & Compliance | Communicates with regulatory bodies, following mandated reporting requirements. | Name  Phone  Email |
| Human Resources | Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees. | Name  Phone  Email |
| Regulatory Contacts | Receives information about a breach according to timeline and format mandated by regulatory requirements. | Name  Phone  Email |
| **COMMUNICATIONS** | | |
| Marketing & Public Relations Lead | Communicates externally with customers, partners and the media.  Coordinates all communications and request for interviews with internal subject matter experts and security team.  Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach. | Name  Phone  Email |
| Web & Social Media Lead | Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users.  Sets up monitoring across social media channels to ensure we receive feedback or questions sent by customers through social media. | Name  Phone  Email |
| Technical Support Lead (Internal) | Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes. | Name  Phone  Email |
| Technical Support Lead (External) | Provides security bulletins and technical guidance to external users in case of a breach. | Name  Phone  Email |

**THREAT CLASSIFICATION**

*In your incident response plan, include information on how you evaluate risk. You may develop your own threat classification or risk ranking system to determine the level of incident response necessary. We have included the sample system below as a guideline.*

The CIA Triad (Confidentiality, Integrity, and Availability) is a framework for incident classification that helps to prioritize the level of incident response required for a cyber attack. CIA is as follows:

1. **Confidentiality** – Incidents involving unauthorized access to systems, including privileged account compromise. The more confidential the data or the more important the systems are to the business, the higher the potential impact.
2. **Integrity** – Incidents involving data poisoning, including leveraging a privileged account to corrupt or modify data. The more sensitive the data, the higher the potential impact.
3. **Availability** – Incidents that impact the availability or proper functioning of services, such as Distributed Denial of Service (DDoS) or ransomware, including use of privileged accounts to make unauthorized changes. The more critical the services to the business, the higher the potential impact.

When ranking the level of risk to the organization and the type of incident response required, you must take into account the extent to which privileged accounts are compromised, including those associated with business users, network administrators, and service or application accounts. When privileged accounts are involved in the breach, the level of risk increases exponentially as does the response required.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sample Cyber Incident | CIA category | Privileged Account Breach | Business Impact | Risk Level |
| An employee shares information with an unauthorized third party, but the information is not personal or protected by regulatory requirements. | C | No | Low | Low |
| Malware hidden within a program leverages local credentials to execute but access privileges of the network administrator. Adware appears on the computer. | C, I | Yes | Low | Medium |
| A cyber criminal uses a pass-the-hash technique to steal passwords and access multiple databases and root accounts. | C | Yes | High | High |
| The cyber criminal uses privileged access to overwhelm the system with requests, slowing performance and damaging the user experience. | C, I, A | Yes | High | High |

**[COMPANY NAME] COMPLIANCE AND LEGAL OBLIGATIONS**

*As part of your incident response plan, document the legal and compliance reporting requirements your company must meet. This way, you can respond immediately to an incident, instead of having to go through legal discovery or check if reporting is required while you are in the middle of a crisis.*

*See the Appendix for a list of regulations that may impact your business. It is important you review with your legal counsel to ensure a complete list that applies to you.*

**ACTIONS TAKEN DURING INCIDENT RESPONSE**

*Below is a sample reporting template to use for documenting the steps and documentation gathered during your review and response to a cyber incident involving privileged accounts. Make updates to reflect your approved process and the tools you use. Add a responsible party for each step now, so everyone knows what data they need to gather and steps to take when an incident happens.*

To demonstrate and improve the effectiveness of [Company Name] incident response team and security tools, [Company Name] requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

Below is the reporting checklist to use when documenting actions taken to combat a high-level privileged account attack. At [Company Name], it is our goal to meet compliance requirements and prioritize business continuity to minimize impact and cost.

|  |  |  |  |
| --- | --- | --- | --- |
| Phase of Cyber Incident | Action | Team Member/System | Day/Time  Action Taken |
| **Incident Discovery and Confirmation** | Describe how the team first learned of the attack (security researcher, partner, customer, auditor, internal security alert, etc.) |  |  |
| Analyze audit logs to identify unusual or suspicious account behavior that indicates a likely attack and confirm attack has occurred. |  |  |
| Describe potential attacker, including known or expected capabilities, behaviors, and motivations. |  |  |
| Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party. |  |  |
| Prepare an incident timeline to keep in ongoing record of when the attack occurred and subsequent milestones in analysis and response. |  |  |
| Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites. |  |  |
| Evaluate extent of damage upon discovery and risk to systems and privileged accounts in particular. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. |  |  |
| Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered. |  |  |
| Diagram the path of the incident/attack to provide an “at-a-glance” view from the initial breach to escalation and movement tracked across the network |  |  |
| Collect meeting notes in a central repository to use in preparing communications with stakeholders |  |  |
| Inform employees regarding discovery. |  |  |
| Analyze incident Indicators of Compromise with threat intelligence tools |  |  |
| Share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach in order to increase your chances of catching the attacker. If so, make sure that aligns with your compliance requirements. |  |  |
| **Containment and Continuity** | Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems. |  |  |
| Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media. |  |  |
| Force multi-factor authentication or peer review to ensure privileges are being used appropriately. |  |  |
| Change passwords for all users, service, application, and network accounts. |  |  |
| Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker. |  |  |
|  | Remove systems from production or take systems offline if needed. |  |  |
| Inform employees regarding breach containment. |  |  |
| Analyze, record and confirm any instances of potential data exfiltration occurrences across the network |  |  |
| Share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |
| **Eradication** | Close firewall ports and network connections. |  |  |
| Test devices and applications to be sure any malicious code is removed. |  |  |
| Compare data before and after the incident to ensure systems are reset properly. |  |  |
| Inform employees regarding eradication. |  |  |
| Share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |
| **Recovery** | Download and apply security patches. |  |  |
| Close network access and reset passwords. |  |  |
| Conduct vulnerability analysis. |  |  |
| Return any systems that were taken offline to production. |  |  |
| Inform employees regarding recovery. |  |  |
| Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |
| **Lessons Learned** | Review forensic evidence collected. |  |  |
| Assess incident cost. |  |  |
| Write an Executive Summary of the incident |  |  |
| Report to executive team and auditors if necessary. |  |  |
| Implement additional training for everyone involved in incident response and all employees. |  |  |
| Update incident response plan. |  |  |
| Inform employees regarding lessons learned, additional training, etc. |  |  |
|  | Share information externally (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |

**APPENDIX**

*This Appendix is optional and should be deleted before you distribute this security policy to your organization.*

**APPENDIX A**

**COMPLIANCE AND LEGAL OBLIGATIONS**

*Below is a list of regulations that include requirements for incident response, including preparation, documentation, and reporting. Select the requirements that apply to your organization, include the appropriate contacts in the contact section of this template, and make sure the actions and tools you have in place provide the capabilities to meet your obligations.*

**INDUSTRY-SPECIFIC REGULATIONS**

**HIPAA and HITECH**

Any organization that creates, receives, maintains, or transmits electronic protected health information (ePHI) in the United States must meet HIPAA requirements for access control and data sharing.

* **Reporting requirements –** The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
* Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.
* **Learn more –** <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

**PCI DSS**

PCI DSS provides organizations that accept, store or transmit credit card data with guidelines for privilege management and a framework to protect cardholder data.

* **Reporting requirements –** PCI DSS requires entities have an incident response plan and alert effected parties immediately. [PCI DSS 3.2.1](https://www.pcisecuritystandards.org/document_library), released on May 2018, marks the latest version.
* You may want to set up an arrangement with an independent Payment Card Industry Forensic Investigator (PFI) to call if you need outside expertise.
* **Learn more –** <https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf>

**FISMA/NIST**

FISMA is United States legislation intended to protect the security, confidentiality, and integrity of government data systems. A FISMA audit is a test of an organization’s system against the controls outlined in various NIST publications such as NIST SP 800-53, NIST SP 800-171, FIPS 199, and FIPS 200.

* **Reporting requirements –** A FISMA audit is a test of an organization’s system against the controls outlined in various NIST publications such as NIST SP 800-53, NIST SP 800-171, FIPS 199, and FIPS 200.
* **Learn more –** <https://csrc.nist.gov/projects/risk-management>

**NERC/CIP**

The NERC Critical Infrastructure Protection (CIP) Standards apply to the cyber security aspects of the Bulk Electric System and its efficient and reliable supply.

* **Reporting requirements –** Reliability standards require the reporting of cyber security incidents that compromise, or attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).
* **Learn more –** <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

**SOX**

Sarbanes-Oxley (SOX) is designed to reduce corporate fraud by requiring an increase in the strength and granularity of security controls for financial auditing and reporting.

* **Reporting requirements –** Companies must disclose failure of security safeguards and security breaches to SOX auditors.
* **Learn more –** https://www.sarbanes-oxley-101.com/

**NYCRR**

One of the strictest cyber security regulations at a federal or state level, NYCRR applies to New York insurance companies, banks, and other regulated financial services institutions, including agencies and branches of non-US banks licensed in the state of New York.

* **Reporting requirements –** Documentation and reporting regarding cyber security events and related incident response activities are required.
* **Learn more –** [https://www.dfs.ny.gov/industry\_guidance/cyber\_faqs#](https://www.dfs.ny.gov/industry_guidance/cyber_faqs)

**GEOGRAPHIC REGULATIONS**

**EU GDPR**

Any organization dealing with EU citizens' Personally Identifiable Information is obligated to meet standards for effective data protection, adequate security measures, and privacy by design to comply with EUGDPR.

* **Reporting requirements –** Under GDPR, breach notification is mandatory in all member states where a data breach is likely to result in a risk for the rights and freedoms of individuals. This must be done within 72 hours of first having become aware of the breach. Data processors are required to notify their customers, the controllers, without undue delay after first becoming aware of a data breach.
* **Learn more –** <https://www.eugdpr.org/key-changes.html>

**UK Cyber Essentials**  
Contractors in the UK that handle sensitive or personal information must receive Cyber Essentials Certification to demonstrate understanding and enforcement of privilege management.

* **Reporting requirements –** UK Cyber Essentials uses external auditors to confirm compliance with the security framework and award certificates.
* **Learn more –** <https://www.cyberessentials.ncsc.gov.uk/>

**UAE NESA**

The National Electronic Security Authority (NESA) in the United Arab Emirates requires government entities and businesses in critical sectors closely control and protect privileged accounts.

* **Reporting requirements –** NESA compliance involves a maturity-based self-assessment and allows for external auditing, testing and even intervention if activities pose a significant threat to national security.

**Appendix B**

*Having a documented incident response plan is a great first step. Now you need to ensure your team has the right tools to support the actions called for in the plan.*

*Below is a table listing the incident response phases in this plan that can be implemented using Privilege Management solution, including Secret Server, Privilege Manager, and Privileged Behavior Analytics. As part of your defense-in-depth strategy, Delinea lets you contain a cyber incident and fix the problem while you continue normal business operations.*

|  |  |
| --- | --- |
| Incident Response Phase | Incident Response Actions Supported by Delinea |
| **Incident Discovery and Confirmation** | * Automatically detect privilege account activity that is out of the ordinary, compared with a baseline. * Trigger real-time alerts of suspicious behavior regarding privileged accounts and send them to an incident response team for further investigation and action. * Quickly determine the extent of an incident by auditing which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. It’s also possible to take a snapshot of the audit logs for comparison. * Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites using real-time threat intelligence. |
| **Containment and Continuity** | * Ensure your incident response team has the permissions and privileges required to carry out an investigation and * Enable additional, temporary permissions if needed for the technical and security teams to quickly access and monitor systems. * Immediately and automatically change passwords for all users, service, application, and network accounts – without stopping them from accessing systems they need to do their job. * Increase monitoring of privileged accounts and systems by restricting access to sensitive systems, requiring additional approval processes for privileged access or forcing multi-factor authentication for privileged accounts. * Increase the sensitivity of application security controls (allowing, deny, and restrict) to prevent malicious malware from being distributed by the attacker. |
| **Eradication** | * Compare data before and after the incident with easily customized reports so you can quickly determine which privileged accounts might be malicious and audit their lifecycle. * Monitor and audit all activity for privileged accounts to determine that they are back to normal expected usage, paying special attention to all third parties, including temporary workers, contractors, and partners |
| **Recovery** | * Operate security controls with lower sensitivity for a period of time or shut down those accounts entirely until you are confident systems have fully recovered. * See all activity at a glance in a centralized dashboard so you and your leadership team can feel confident that the most critical systems and data are protected and back to normal. * Easily create reports and share with executives and auditors to demonstrate how people and tools responded to an incident without manually checking through your logs. |
| **Lessons Learned** | * Get a clear picture of what worked and what needs improvement. * Quickly change settings to reflect new policies and requirements. |

**About Delinea**

Delinea is a leading provider of privileged access management (PAM) solutions for the modern, hybrid enterprise. We make privileged access more accessible by eliminating complexity and defining the boundaries of access to reduce risk, ensure compliance, and simplify security. Delinea empowers over 14,000 customers worldwide, including over half the Fortune 100. Our customers include the world’s largest financial institutions, intelligence agencies, and critical infrastructure companies. delinea.com