Company Logo

Info-Tech Research Group

Security, Risk & Compliance

**Security Incident Management Runbook: Data Breach**

Last revised: MM/DD/YY

## Contents

[Contents 2](#_Toc4574927)

[Revision History 2](#_Toc4574928)

[Introduction 3](#_Toc4574929)

[Incident Assessment Methodology 3](#_Toc4574930)

[Impact 3](#_Toc4574931)

[Scope 3](#_Toc4574932)

[Threat Escalation Protocol 4](#_Toc4574933)

[Threat Escalation Protocol 4](#_Toc4574934)

[Incident Management Summary 5](#_Toc4574935)

[Incident Response Workflow 6](#_Toc4574936)

[Response Procedures 7](#_Toc4574937)

[Detection Phase 7](#_Toc4574938)

[Analysis Phase 8](#_Toc4574939)

[Containment Phase 11](#_Toc4574940)

[Eradication Phase 13](#_Toc4574941)

[Recovery Phase 14](#_Toc4574942)

[Post-Incident Phase 16](#_Toc4574943)

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Change** | **Author(s)** | **Date of Change** |
| 1.0 | Initial Draft |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

Effective and efficient incident management involves a formal process to detect, analyze, contain, eradicate, recover, and conduct post-incident activities. This runbook provides detailed procedures that govern the incident management process to handle **data breach** incidents.

# Incident Assessment Methodology

The incident assessment methodology consists of the evaluation of impact, scope, and threat escalation.

## Impact

The evaluation of the effects of a data breach on business functions, data, and recovery efforts. Incident impact should be prioritized based on the below factors. [To be completed by and catered to the member organization. Below is an example.]

1. The current and future functional impact on any business function or operation.
2. The informational impact as it relates to the confidentiality, integrity, and availability of data.
3. The time and required resources needed to recover from the incident.

|  |  |
| --- | --- |
| **Data Breach Impact Criteria** | |
| **Rating** | **Definition** |
| High | A data breach that exposes highly sensitive and/or regulated data (e.g. PII, PHI, PCI data, trade secrets), is likely to impose major costs on the organization (both monetary and reputational), and may interrupt business continuity. |
| Medium | A data breach that exposes internal/confidential data that is damaging to the organization, but there are no regulatory or legal implications. |
| Low | A data breach that exposes data that is otherwise public or subject to open records requests. The confidentiality of the data is not necessarily the concern, but the manner in which it was obtained warrants a security incident. |

## Scope

The evaluation of the effects on information technology (IT) systems. IT systems incident scope is a critical component that aids in decision making throughout the incident management process. Incident scope should be prioritized based on the below factors. [To be completed by and catered to the member organization. Below is an example.]

|  |  |
| --- | --- |
| **Data Breach Scope Criteria** | |
| Rating | Definition |
| High | ≥100 records exfiltrated |
| Medium | 11-99 records exfiltrated |
| Low | ≤10 records exfiltrated |

### 

## Threat Escalation Protocol

A threat escalation protocol is used to define the type of stakeholders needed during the incident management process. Informing and consulting these stakeholders during the incident management process is crucial when defending the organization against a data breach. A threat escalation protocol clearly defines escalation procedures for data breach incidents. [To be completed by and catered to the member organization. Below is an example.]

**Table 1. Threat Escalation Protocol**

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Escalation Protocol** | | | |
| **Impact** | **Scope** | | |
| **High** | **Medium** | **Low** |
| **High** | Tier 1 | Tier 1 | Tier 2 |
| **Medium** | Tier 1 | Tier 2 | Tier 2 |
| **Low** | Tier 2 | Tier 2 | Tier 3 |

### Threat Escalation Protocol

Below is the threat escalation protocol that will be used when dealing with data breach incidents.

|  |  |  |
| --- | --- | --- |
| **Threat Escalation Protocol** | **Criteria** | **Stakeholders** |
| **Tier 1** | * High impact, high scope * High impact, medium scope * Medium impact, high scope | * End User * Help Desk * Cybersecurity * IT Operations * CISO * Legal, HR, PR * Senior Management * External Third Parties |
| **Tier 2** | * High impact, low scope * Medium impact, medium scope * Medium impact, low scope * Low impact, high scope * Low impact, medium scope | * End User * Help Desk * Cybersecurity * IT Operations * CISO |
| **Tier 3** | * Low impact, medium scope * False positive | * End User * Help Desk * Cybersecurity |

# Incident Management Summary

The table below includes the definition of data breach, the effects of a data breach on your organization, and a summary of the response required to deal with this incident.

|  |  |
| --- | --- |
| **What Is the Incident?** | A data breach occurs when an organization’s records are exposed through an internal error or an attack perpetrated by a hostile third party or malicious insider. A data breach commonly involves sensitive data (e.g. PII), but loss of such data is not required for a data breach to have taken place. |
| **Why Should We Care?** | A data breach can cause huge financial and reputational damage, as well as legal implications. These costs are often enough to force small organizations out of business. |
| **How Do We Respond?** | During data breach incidents, stakeholders defined in the threat escalation protocol work collaboratively throughout the entire incident management process.  Consult Info-Tech’s ***Data Breach Reporting Requirements*** document for protocols for regulations such as GDPR, HIPAA, PCI, PIPEDA.  Major activities that take place during data breach incidents include the following:   1. **End Users:** Report any known or suspected data breaches to help desk. 2. **Help Desk:** Interact directly with the end user to gather incident-related information, create and update tickets, and coordinate with the end user throughout the incident management process. 3. **MSSP/Security Operations:** Monitor perimeter security events, analyze logs, conduct open-source intelligence research, provide security event analysis, escalate events to cybersecurity team, implement data breach mitigation service, and open an incident record. 4. **Cybersecurity:** Enrich security event escalations, analyze internal logs, gather evidence, conduct open-source intelligence research, provide technical support, identify any control weaknesses, coordinate all incident activities, and document root cause and investigative activities in an incident record. 5. **IT Operations:** Provide server event support, analyze server logs, conduct open-source intelligence research, isolate any targeted servers, remove from the network, and restore servers, applications, and services. 6. **CISO:** Notify and coordinate with the relevant stakeholders and senior management, evaluate control weaknesses, update policies, recommend the enactment of data breach mitigation services, and facilitate any post-incident activities. 7. **Legal, HR, PR:** Evaluate any brand/reputational damage, determine regulatory compliance violations, conduct any employee disciplinary actions, and facilitate any external reporting. 8. **Senior Management:** Approve any proposed control strategy and allocate budget or resources, and approve any data breach mitigation services. 9. **External Third Parties:** Provide incident investigative support, and share information. |

# Incident Response Workflow

The workflow diagram below outlines the incident management process from detection to post-incident activities, including the responsibilities of each stakeholder in each phase. The workflow outlines the decisions, actions, and pre-established processes that are required to deal with the incident at each stage, for all three threat magnitudes.

## 

# Response Procedures

The actions required to deal with a data breach are detailed below for each relevant stakeholder (team), in each of the six phases (detection, analysis, containment, eradication, recovery, and post-incident).

## Detection Phase

During the detection phase, teams will evaluate a potential data breach incident, for example, suspicious log activity suggesting that an attacker may have penetrated security systems or a user reporting a known accidental sending of sensitive data. Once an incident has been detected, a help desk ticket or incident record/ticket is opened to initiate the detection phase.

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Description | Questions | Action |
| Detection: End User | During the detection phase, the end user will report a potential data breach. | * Did I send an email to the wrong recipient? * Did I leave sensitive data in a public location? * Am I aware of some other breach of data? | * Report a known or suspected breach of data. |
| Detection: Help Desk | During the detection phase, help desk staff will monitor calls and submit tickets. | * Are any end users experiencing incidents that may indicate data was sent out to an unauthorized recipient or compromised in some other way? * Are any users experiencing incidents that may be a diversion associated with a data breach attack (e.g. DDoS attack to cover a data breach)? | * Open a help desk ticket. |
| Detection: MSSP/Security Ops | During the detection phase, MSSP/security operations analysts monitor SIEM, DLP, firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway, and other **events,** and escalate **incidents** to the cybersecurity team. | * Are there indications of a data breach on the network?   E.g.   * DLP alert. * Security system malfunctions or errors. * Presence of unusual IP addresses. * Suspicious activity in logs. | * Review SIEM correlation events. * Review DLP events. * Review a firewall event or series of events. * Review an IDS/IPS event or series of events. * Review a web proxy suspicious connection or series of connections. * Review an antivirus event or series of events. * Review an anti-malware event or series of events. * Review an email gateway event or series of events. * Open or generate an incident record. |
| Detection: Cybersecurity | During the detection phase, cybersecurity staff monitor for events being escalated by the MSSP/security operations. | * Are there indications of a data breach on the network? * Are there any DLP, SIEM, FW, other alerts indicating a loss/transfer of data to an unauthorized party? | * Monitor the incident management system to detect any events that have been escalated. * Open an incident record as appropriate. |
| Detection: IT Operations | During the detection phase, IT operations staff will monitor alerts. | * Are there indications of a data breach on the network? * Are there any DLP, SIEM, FW, other alerts indicating a loss/transfer of data to an unauthorized party? * Are any servers, applications, or services unavailable | * Monitor server, application, and service availability. * Report to cybersecurity. |
| Detection: CISO | No incident management responsibilities. |  |  |
| Detection: Legal, HR, PR | No incident management responsibilities. |  |  |
| Detection: Senior Management | No incident management responsibilities. |  |  |
| Detection: External | No incident management responsibilities. |  |  |

## Analysis Phase

During the analysis phase, teams will analyze the incident to determine the impact of the threat. Depending on the impact, a number of teams will be involved in the remediation of the data breach incident, and the notification of the threat will be escalated as appropriate.

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Description | Questions | Action |
| Analysis: End User | No incident management responsibilities beyond answering incident-related questions. |  |  |
| Analysis: Help Desk | During the incident management analysis phase, help desk staff directly interact with any end users to provide relevant communications and/or updates. | * What updates need to be sent to the end users? | * Open additional help desk tickets as appropriate. * Facilitate end-user notifications. * Close help desk ticket, as appropriate (if false positive). |
| Analysis: MSSP/Security Ops | During the incident management analysis phase, MSSP/security operations staff will continue to monitor SIEM, firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway events, escalate any additional **incidents,** and share answers to incident-related questions with the cybersecurity team. | * What type of data is breached? * What is the source of the breach (e.g. phishing, insider activity, malware)? * What tactics or exploits are being used to breach systems? * What threat actors (nation state, cybercriminals, hacktivists, or cyber extremists) are behind the data breach? * Does the organization need to enact data breach mitigation services to sustain the attack? | * Share threat intelligence with appropriate teams. * Recommend the enactment of data breach mitigation. * Escalate additional events to cybersecurity team. |
| Analysis: Cybersecurity | During the incident management analysis phase, cybersecurity staff will enrich events escalated by MSSP/security Ops by analyzing and correlating internal log data. | * Are the events false positives? * What is the business impact if true data beach? * What is the scope of the data breach and what records were affected? * Which stakeholders were affected? * Where was the data breached from (e.g. USB drive, network drive, cloud app)? * Was the data breach accidental or an attack by a malicious third party? * What was the date and time of the data breach? * Is the exploited vulnerability or compromised credentials still a risk? | * Publish corporate-wide situational awareness alerts to inform end users of any system outages. * Work with Internal Communications, HR, Legal, and PR to determine any breach notification requirements. * Determine which IP addresses link to the attack through logs. * Identify any other potential points of failure (e.g. router, switches, firewalls). * Identify which business functions will be impacted by the data breach. * Continue gathering evidence. * If significant, notify CISO. |
| Analysis: IT Operations | During the incident management analysis phase, IT operations staff will analyze any appropriate server, router, firewall, and application logs, conduct open-source intelligence research, provide technical support, ask incident-related questions, take actions, and document findings in the incident record. | * Where was the data breached from (e.g. USB drive, network drive, cloud app)? * How are end-user facing servers, applications, or services affected? | * Determine which servers are exposed and the potential risk implications. * Assess the implications for any public-facing services. * Maintain a dynamic and frequently updated listing of active server ports. * Determine any impact to servers, applications, or services. * Review relevant server, router, firewall, and application logs to help determine the attack vector and exploited vulnerability. |
| Analysis: CISO | During the incident management analysis phase, CISO will notify and coordinate with the relevant stakeholders and senior management. | * Has a crime been committed? * Are any business servers, applications, or services impacted? * Does a disaster recovery plan need to be enacted? * Is there motive behind the attack? * Which stakeholders need to be notified? | * Approve any corporate-wide situational awareness alerts to inform end users of any system outages. * Approve the disaster recovery enactment plan, if necessary. * Report any external criminal activities to senior management. * Engage with HR, Legal, and PR, as appropriate. * Inform senior management and other stakeholders, as appropriate. * Examine potential reason/motivation for the attack. * Assess if the incident poses a real risk of significant harm. If so, contact law enforcement. |
| Analysis: Legal, HR, PR | During the incident management analysis phase, legal, HR, and PR staff will analyze any insider activity and brand or reputational damage. | * Are there any regulatory, legal, or compliance requirements? * Was there any insider activity? * Was there any brand or reputational damage? | Legal:   * Determine if any regulatory, legal, or compliance mandates have been violated or impacted. * Consult Info-Tech’s ***Data Breach Reporting Requirements*** document for protocols for regulations such as GDPR, HIPAA, PCI, PIPEDA. * Determine if any breach notifications are required (e.g. 72 hours to notify for GDPR). * Consult cyber insurance, if applicable.   PR:   * Determine if any public reputational or brand damage has occurred.   HR:   * If insider activity, consult user’s manager and begin disciplinary actions, if appropriate. |
| Analysis: Senior Management | During the incident management analysis phase, senior management will notify and coordinate with the relevant stakeholders. | * Was there any brand or reputational damage? * Has a crime been committed? * Has data been lost, and does a disaster recovery plan need to be enacted? | * Provide an incident summary/update to the board of directors. * Approve reporting crime to law enforcement. * Approve communication of any incident information with external parties. |
| Analysis: External | No incident management responsibilities. |  |  |

## Containment Phase

During the containment phase, teams will aim to isolate the affected systems and block the attacker’s access to the network.

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Description | Questions | Action |
| Containment: End User | No incident management responsibilities. |  |  |
| Containment: Help Desk | During the incident management containment phase, help desk staff will maintain communications with any impacted end users. | * Do any end users need to be notified? | * Maintain communications with any impacted end users. |
| Containment: MSSP/Security Ops | No incident management responsibilities. |  |  |
| Containment: Cybersecurity | During the incident management containment phase, cybersecurity staff will provide coordination support. | * Is the breach currently on-going? * What is the source of the breach? * Are there indications of other, related incidents? (e.g.: ransomware) * Are there any systems that need to be taken offline? * Do system logs suggest other data has been breached? | * Provide incident coordination support. * Contact vendor for possible assistance in remediation of the event. * Disable breached accounts, if necessary. * Update other system passwords. * Isolate any additional sensitive data to protect against possible recurrent attacks. |
| Containment: IT Operations | During the incident management containment phase, IT operations will prevent the breach from spreading. | * What is the nature of the breach? If malicious, what can stop the breach from reoccurring? | * Close all unnecessary server ports/services and adopt the principle of least privilege. * Block malicious IPs. * Disable breached accounts and shared passwords, if necessary. |
| Containment: CISO | During the incident management containment phase, the CISO will evaluate any containment decisions that affect business practices and provide recommendations. | * Will containment measures affect business practices? | * Provide senior management with incident updates. * Approve systems potentially being taken offline, if necessary. |
| Containment: Legal, HR, PR | During the incident management containment phase, legal, HR, and PR staff will evaluate if any public relations or legal actions need to be taken. | * Are there any legal requirements or notification requirements? * Does the public need to be informed? * Does any reputational damage need to be contained? * Do affected stakeholders need to be notified as per GDPR requirements? * Do affected stakeholders need to be notified as per PIPEDA requirements? | * Take any appropriate action to inform legal agencies. * Use a PR campaign to reduce reputational damage as appropriate. * Consult Info-Tech’s ***Data Breach Reporting Requirements*** document for protocols for regulations such as GDPR, HIPAA, PCI, PIPEDA. * Notify affected stakeholders without undue delay, provide them with plain-language summary of the incident, contact information for DPO, explain likely consequences of the data breach, and what efforts are underway to remediate the incident. * Notify affected stakeholders as soon as possible after confirming the breach, inform them of the following: * Circumstances of the breach. * Date and time of breach (or best approximation). * Description of the affected personal information (to the best of your knowledge). * Steps being taken to minimize potential effects on stakeholders. * Steps stakeholders can take to minimize risks. * Contact information if stakeholders need assistance. |
| Containment: Senior Management | During the incident management containment phase, senior management will determine if any core business function is impacted. | * Has the incident impacted any core business functions? * Has any brand or reputational damage occurred? | * Determine if any additional stakeholders need to be notified. |
| Containment: External | No incident management responsibilities. |  |  |

## Eradication Phase

During the eradication phase, teams will restore applications, servers, and services. After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Description | Questions | Action |
| Eradication: End User | No incident management responsibilities. |  |  |
| Eradication: Help Desk | During the incident management eradication phase, help desk staff will maintain communications with impacted end users. | * Does the end user need to be notified? | * Maintain communications with any impacted end users. |
| Eradication: MSSP/Security Ops | No incident management responsibilities. |  |  |
| Eradication: Cybersecurity | During the incident management eradication phase, cybersecurity staff will eliminate the root cause of the incident. | * Has the root cause of the breach been addressed? * Are there other incidents that resulted from the data breach? | * Provide incident coordination support. * If data is exfiltrated due to malware, work with IT operations to disable/remove malware. * Update security controls (e.g. tighten DLP rules). |
| Eradication: IT Operations | During the incident management eradication phase, IT operations staff will restore data, expand the network, and identify defense gaps in the organization. | * Does malware need to be removed? * Are all potentially compromised passwords reset? * Are there any control gaps that allowed this incident to occur? * Do servers need to be reconfigured to prevent recurrence? | * If data is exfiltrated due to malware, work with cybersecurity to disable/remove malware. * If data is breached due to phishing, ensure sender is blocked. * Consult logs to investigate whether an attacker gained access to other systems, elevated other privileges, etc. * Identify and address vulnerability, and patch systems as necessary. * Inform the CISO of any organizational defense control gaps. |
| Eradication: CISO | During the incident management eradication phase, the CISO will develop any control weakness strategies, as appropriate. | * Do any new controls need to be implemented? * Do any controls need to be updated? | * Approve new controls and the updating of existing ones. |
| Eradication: Legal, HR, PR | During the incident management eradication phase, legal, HR, and PR staff will evaluate if any public relations or legal actions need to be taken. | * Are there any legal requirements or notification requirements? * Are disciplinary actions being carried out? | * Legal: Continue breach notifications, as required. * HR: If data breach was due to a rogue user, ensure disciplinary actions are considered and implemented. |
| Eradication: Senior Management | During the incident management eradication phase, senior management will approve the proposed control strategy and allocate any budget or resources to eradicate. | * Do budget or resources need to be assigned? | * Approve the control weakness strategy. * Allocate budget and resources for eradication. |
| Eradication: External | No incident management responsibilities. |  |  |

## Recovery Phase

During the recovery phase, teams will enact processes and procedures for recovery and full restoration of any affected applications, servers, and services during the incident. In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g. firewall rulesets, boundary router access control lists).

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Description | Questions | Action |
| Recovery: End User | No incident management responsibilities. |  |  |
| Recovery: Help Desk | During the incident management recovery phase, help desk staff will maintain communications with impacted end users. | * Does the end user need to be notified? | * Maintain communications with any impacted end users. |
| Recovery: MSSP/Security Ops | No incident management responsibilities. |  |  |
| Recovery: Cybersecurity | During the incident management recovery phase, cybersecurity staff will document any findings in an incident report. | * Is the incident report comprehensive enough? * Are operations back to normal? | * Validate systems are back to regular operations. * Confirm that any data lost has been restored. * Update incident record. |
| Recovery: IT Operations | During the incident management recovery phase, IT operations staff will ensure that all applications, servers, and services are back online and restored. | * Has all data been restored? * Have all systems returned to normal operation? | * Restore data, if necessary. (Consult data owners to ensure proper state of data before restoring.) * Scan systems to ensure operations are back to normal. |
| Recovery: CISO | During the incident management recovery phase, the CISO will evaluate any weaknesses in security controls or policies as appropriate. | * Do any controls or policies need to be updated? | * Review any security policies or controls, as appropriate. |
| Recovery: Legal, HR, PR | During the incident management recovery phase, legal, HR, and PR staff will determine if all relevant paperwork is complete. | * Does any further documentation need to be completed? * Are additional PR efforts required (e.g. final press release)? | * HR: Ensure appropriate documentation is filled out regarding any malicious or accidental insider activity. * PR: Follow up with communications. * Legal: Continue legal process. |
| Recovery: Senior Management | No incident management responsibilities. |  |  |
| Recovery: External | No incident management responsibilities. |  |  |

## Post-Incident Phase

During the post-incident phase, teams will perform root-cause analysis and lessons-learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement and all related active tickets should be updated and closed. This phase involves performing post-mortem, root-cause analysis, and lessons-learned activities with various teams and stakeholders within the organization.

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Description | Questions | Action |
| Post-Incident: End User | No incident management responsibilities beyond additional awareness and training, if appropriate. |  |  |
| Post-Incident: Help Desk | No incident management responsibilities. |  |  |
| Post-Incident: MSSP/Security Ops | During the incident management post-incident phase, the MSSP/security operations staff will support any post-incident activities, as appropriate. | * Are there any MSSP/security ops processes that need to be improved? | * Participate in any post-incident meetings, as appropriate. |
| Post-Incident: Cybersecurity | During the incident management post-incident phase, cybersecurity staff will support any post-incident analysis and ensure all findings are documented in an incident report. | * Has the incident been resolved and can the incident tickets be closed? | * Document all findings in an incident report. * Provide input to any post-incident analysis. * Update and close incident ticket. |
| Post-Incident: IT Operations | During the incident management post-incident phase, IT operations staff will support any post-incident activities, as appropriate. | * Are there any IT Operations processes that need to be improved? | * Participate in any post-incident meetings, as appropriate. |
| Post-Incident: CISO | During the incident management post-incident phase, the CISO will facilitate any post-incident activities. | * How can the incident response process be improved? | * Conduct and facilitate any post-incident activities/lessons-learned meetings. |
| Post-Incident: Legal, HR, PR | During the incident management post-incident phase, legal, HR, and PR staff will support any post-incident activities, as appropriate. | * Are there any legal, HR, or PR processes that need to be improved? | * Participate in any post-incident meetings, as appropriate. * Update policies. * Update legal, HR, and PR processes based on lessons learned. |
| Post-Incident: Senior Management | During the incident management post-incident phase, senior management will support any post-incident activities, as appropriate. | * Are there any senior management processes that need to be improved? | * Participate in any post-incident meetings, as appropriate. |
| Post-Incident: External | No incident management responsibilities. |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.