INCIDENT RESPONSE PLAN

https://www.linkedin.com/in/joas-antonio-dos-santos/

Purpose

The objective of the Joas Antonio Incident Management Policy is to describe the requirements for dealing with information security incidents.

Audience or interested parties

The Incident Management Policy applies to executive management and other individuals responsible for protecting Joas Antonio Company Information Resources.

summary

Incident Response Plan

Incident Handling Team

An Incident Handling Team (ETI) will be established, consisting of legal experts, risk managers and other department managers who must be involved in decisions related to incident response.

ETI is responsible for:

- Ensure incident response activities are carried out in accordance with legal, contractual and regulatory requirements.
- Internal and external communications related to information security incidents.
- Ensure employees are trained on how to report a potential incident.

Incident Response Team

• The Incident Response Leader will be designated to supervise and direct the incident response activities of the (Company).
• The Incident Response Lead will assemble and oversee a Cybersecurity Incident Response Team (CSIRT).
• CSIRT will respond to identified cybersecurity incidents following the Incident Response Plan.
• The Incident Response Commander is responsible for properly reporting incidents to the CIO/ETI.

Incident response plan

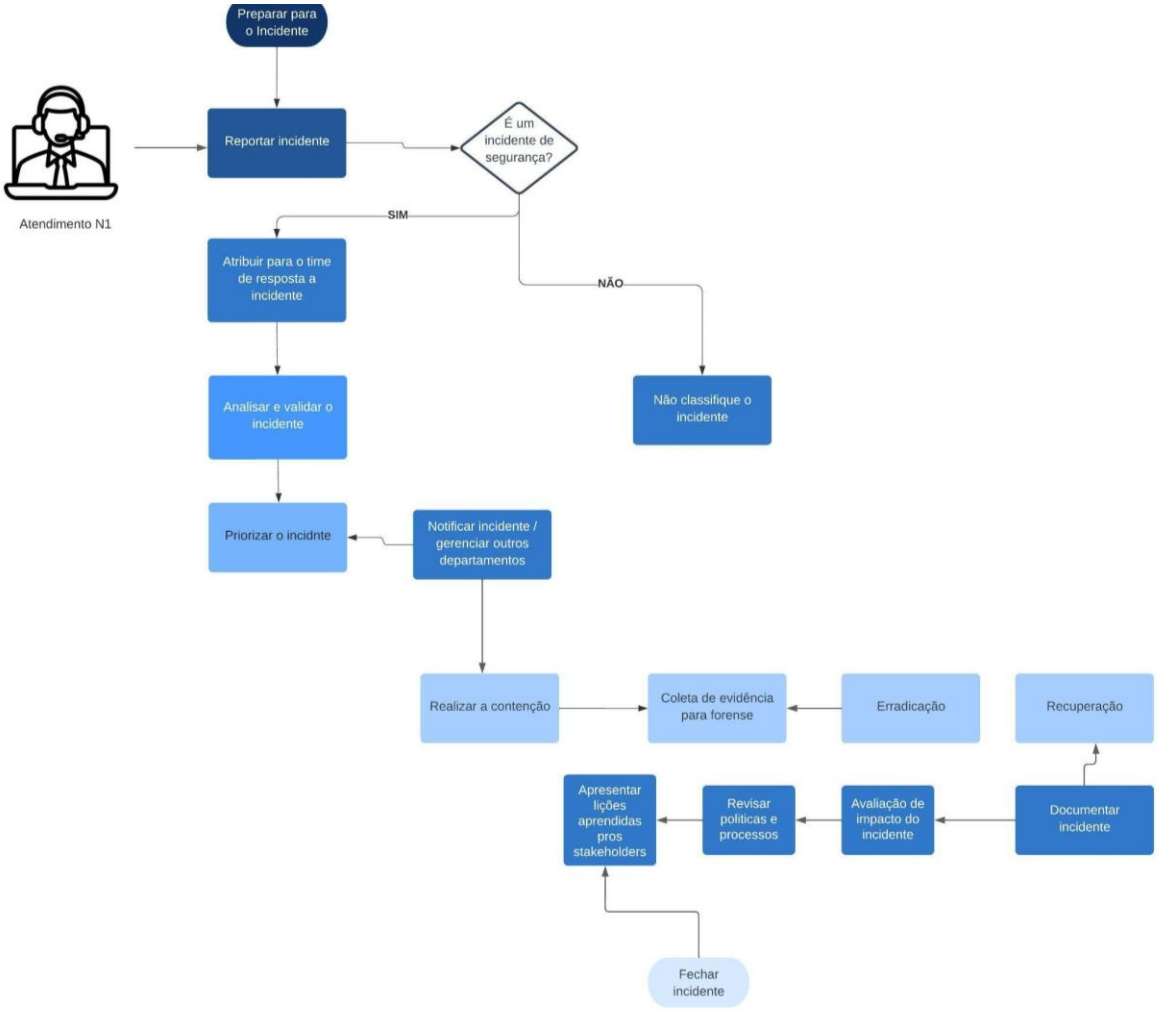
- The Incident Response Leader is responsible for creating, implementing and maintaining the incident response plan.
- The Incident Response Plan must be tested by the CSIRT and ETI annually.

Incident Notification

- Management must provide a means for all personnel to report potential incidents. Reporting methods must ensure that a potential incident is promptly escalated to the appropriate person.
- The SOC is responsible for monitoring event logs, vulnerability management, and other logs for suspicious activity.
- All reported incidents must be evaluated by a member of the CSIRT or ETI to determine the type of threat and activate appropriate response procedures. All members of the CSIRT or ETI should be familiar with how to assess and escalate a potential incident.
- The Incident Response Leader must report the incident to senior leadership.
- Senior leadership must promptly report any potential breaches and/or incidents involving customer data to the Incident Handling Team (ETI).

Incident Response Flow

Incident Response Plan Created by Joas



Step 1 - Incident Response Preparation:

At this stage, the organization prepares to deal with security incidents. This includes developing policies and procedures, identifying an incident response team (CSIRT), implementing monitoring tools and technologies, and conducting training and simulated exercises to ensure the team is ready to act when needed. .

Step 2 - Incident Assignment:

As soon as an incident is detected, the incident response team is activated. Incident attribution involves identifying the type and severity of the incident, determining whether it is an isolated event or part of a broader threat, and assigning the appropriate team to handle the incident.

Step 3 - Incident Triage:

At this stage, the team performs a preliminary analysis of the incident to better understand the nature of the problem. Triage helps determine whether the incident is a real threat, assess its potential impact, and begin collecting relevant information.

Step 4 - Notification:

Notification involves informing relevant stakeholders about the incident, including senior management, IT teams, corporate communications and, in some cases, regulatory authorities. Effective communication during an incident is crucial to ensuring a coordinated response.

Step 5 - Containment:

Once the incident has been identified and assessed, the next step is to contain the threat. This may involve stopping malicious activity, isolating affected systems, and implementing measures to prevent the incident from spreading.

Step 6 - Evidence Collection and Forensic Analysis:

During this phase, the response team collects digital evidence to understand how the incident occurred, who was responsible, and what the impact was. Forensic analysis is crucial to strengthening future security and can be used in legal proceedings.

Step 7 - Eradication:

After forensic analysis, the team works to completely eliminate the threat. This may involve removing malware, patching vulnerabilities, and implementing measures to prevent future instances of the same type of incident.

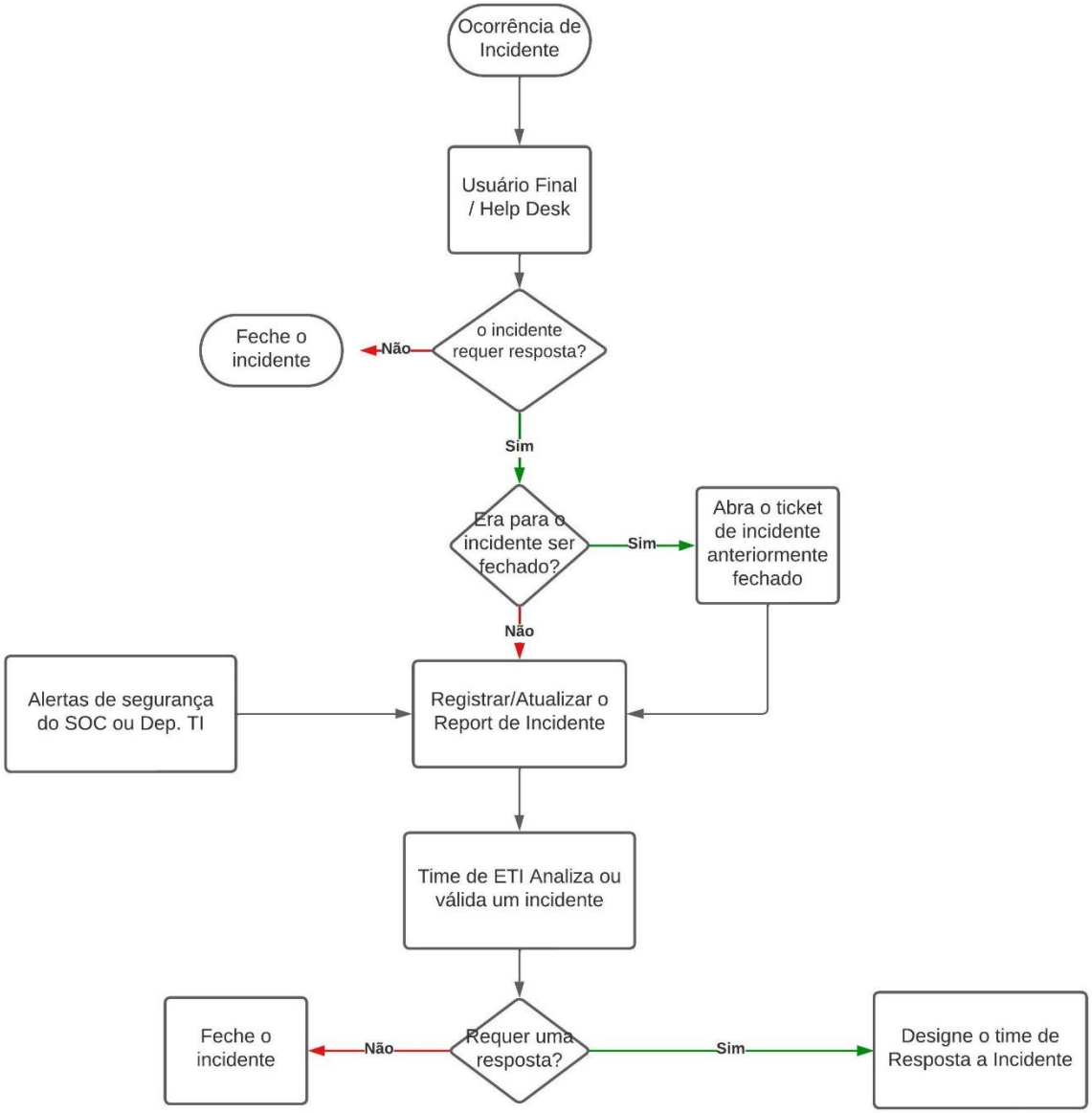
Step 8 - Recovery:

At this stage, the organization strives to return to normal operations. This may include restoring data from backups, rebuilding affected systems, and implementing security improvements to prevent future similar incidents.

Step 9 - Post-Incident:

After the incident has been resolved and normal operation restored, it is crucial to conduct a post-incident review. This involves evaluating the effectiveness of the response, identifying areas for improvement, and documenting lessons learned. This phase is essential to strengthening the organization's security posture in the future.

Incident notification and attribution flow



If an employee identifies abnormal changes or indicators of an incident, he or she should immediately check their database to confirm the changes and inform help desk personnel, such as system or network administrators, of the situation. For our purposes, it's important to note here that a help desk is staffed by experienced incident handlers with years of experience. The help desk will accept such a request from an employee and perform a preliminary analysis to determine whether the employee is reporting a valid intrusion or breach from malicious sources. If the help desk finds that the incident did occur, it will open a case for further investigation. It will then attempt to determine whether the incident reflects previous incidents and conduct additional examinations. If the incident is found to be similar to a previous incident, the help desk will reopen the previously closed incident and update the incident record. Otherwise, it records it by collecting information about the incident, such as security alerts and indicators from the IT department. This incident record is sent to the IR department for analysis and validation. If the IR department deems the incident valid, it will immediately assign the IR team for further analysis.

Incident reporting

ETI is responsible for ensuring that notification and communication, both internally and with third parties (customers, suppliers, law enforcement, etc.), based on legal, regulatory and contractual requirements, occurs in a timely manner.

All information related to an incident is considered confidential, and at no time should any information be discussed with anyone outside of Joas Antonio Company without the approval of senior management and our legal counsel.

People/employees

- Personnel must be notified whenever an incident or incident response activities may impact their work activities.
- Internal communications should aim to avoid panic, prevent the spread of misinformation, and notify personnel of appropriate communication channels.

Interaction with law enforcement authorities

- Interaction between law enforcement and emergency services personnel must be coordinated by the Incident Response Leader or a member of the ETI.
- Legal advisor must be consulted in communications with law enforcement

Customers and Partners

- All customers and partners affected by the incident must be notified in accordance with applicable contractual language, service level agreements (SLAs), statutes and/or applicable regulations.
- Communications with customers and partners must be consistent, delivering the same or similar message to each.

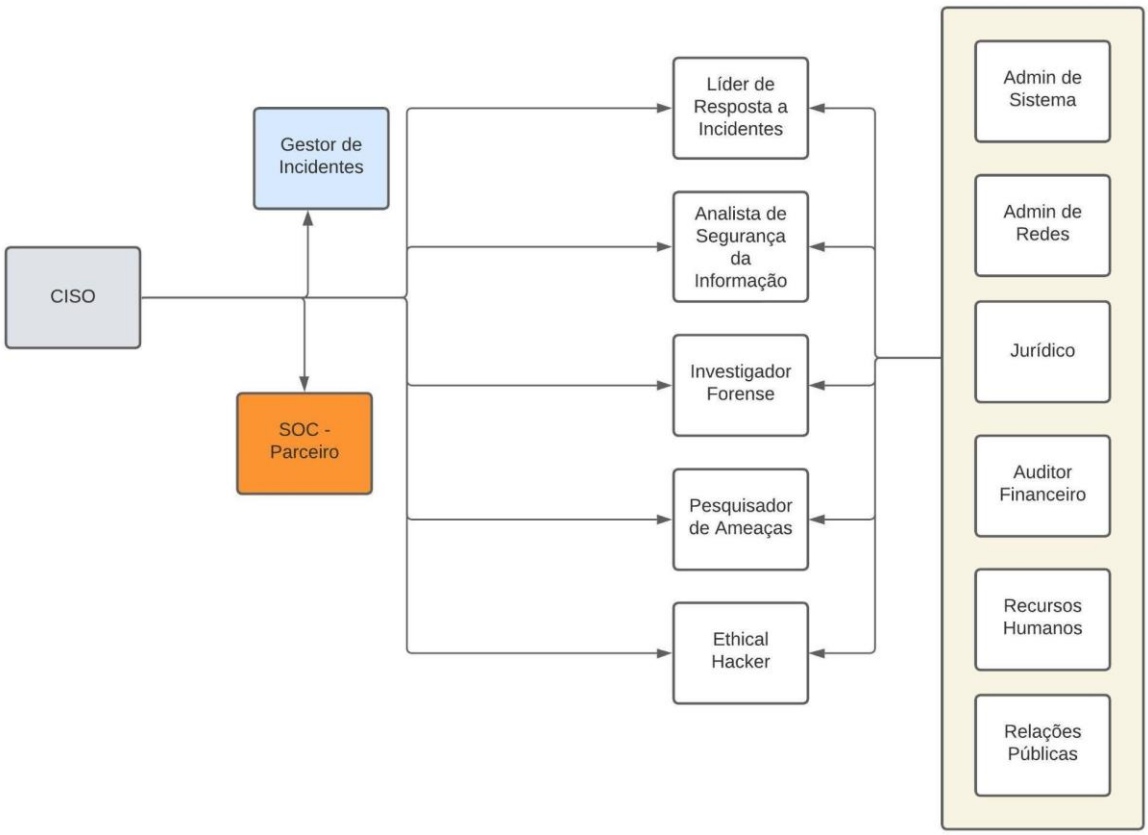
Regulatory Authorities

- Only ETI members are permitted to discuss the nature and/or details of an incident with any regulatory agencies.
- ETI should contact regulators as necessary. (See Appendix IV of the Incident Response Plan)

Public Media

- ETI or senior management will designate a designated spokesperson responsible for communication with the media.
- Inquiries from media agencies should be directed to the designated spokesperson and ETI.

Responsibilities and roles



Incident Management RACI Matrix

Responsible (R - Responsible):

The person or team that is responsible for carrying out the task or activity. They are the ones doing the real work.

Accountable (A - Final Responsible):

The person who is ultimately responsible for the final outcome of the task or activity. They may or may not be the person performing the task, but they are the ones accountable for success or failure.

Consulted (C - Consulted):

The people or stakeholders who need to be consulted or provided information and insights before the decision is made or the task is performed. They are sources of knowledge or experience that can impact the process.

Informed (I - Informed):

People or interested parties who need to be informed about the progress of the task or activity, but who are not directly involved in its execution. They may need to be aware of decisions or outcomes, but they do not need to actively contribute.

STEP	ACTIVITY	SOC N1/N2	Usuário Final / Equipe de TI	Gestor de Service Desk	Cliente	Gerente de Resposta a Incidente	Líder de Resposta a Incidente	Ethical Hacker	Service Desk / Balcão de Atendimentos	Time de GMUD
1	Identificação do Incidente	R	R	R	I	R	A, R	R	A, I	
2	Registro de Incidente	R	A, R	I	I	C	A, R	R		
3	Categorização de Incidente	R	I	C		C	A, R			
4	Priorização de Incidente	R	I	C, I		C	A, R			
5	Atribuição do Incidente	I	C	C, I			A, R			
6	Diagnóstico Inicial de Incidente	R, A	I	A, R			A,C			
7	Gestão de SLA e escalação N2/N3	R		A, R		A,R,C,I	A,C			
8	Escalação Hierarquica	I		I, R			A,C			
9	Investigação e Diagnóstico	I		A,R, I			A,C			
10	Mudanças necessárias?	I	C, I	A,R, I			A,C			I
11	Contenção e Recuperação	I		A,R, I			A,C			I
12	Fechamento de Incidente	R, A	I	A,R, I	I	A,R, I	A,R, I	R	R,C,I	I

Incident Identification

The End User can be anyone in the organization who requests incident resolution or request fulfillment services from the IT organization. Or, the End User can be anyone in the organization who detects and reports an Incident (typically IT Employees).

- The Service Desk role is responsible for having analysts available to contact and be informed of an Incident or Request.
- The Service Desk Analyst is informed and responsible for reporting Incidents and Requests.
- All End Users are responsible for following the contact details and procedures outlined in the Service Catalog for all IT Incident or Request service requests.
- It is the responsibility of all End Users, Customers, IT Employees and IT Management to report all Incidents to the Service Desk, including those where IT staff responses resolve an Incident before End Users are aware (such Incidents are reported for documentation purposes only).

Incident Response Plan Created by Joas

Incident Log

The Service Desk Analyst who accepts the End User/IT Employee contact is responsible and has the obligation to create a Record and record all relevant information. The Service Desk Analyst is also responsible for the following:

- Determine whether the End User/IT Employee is referring to an existing open Record, a Major Incident Master Record, or is reporting a new Incident or Request.
- Update existing Records with all contacts made by the End User / IT Employee. Additional information provided (if relevant) will be evaluated for changes to existing Categories, Priorities and/or Escalations.
- Map all Incidents and Requests to the affected IT Service(s) identified in the Service Catalog.
- In the event that a NEW serious service degradation is detected, immediately inform the Service Desk Manager and continue Categorizing and Prioritizing the Record.
- The Service Desk Manager is informed immediately when a NEW serious service degradation is detected.
- The End User/IT Employee is Consult for a detailed description of the hardware and/or software involved and to provide a brief history of known events leading up to the Incident.
- The Service Desk Analyst will inform the End User/IT Employee of the next steps to be taken.

Incident Categorization

All Open Records are first classified as Incidents or Requests. All Records are further categorized using the Categorization Template, and all Records are related to the affected Services as outlined in the Service Catalog.

- The Service Desk analyst will be responsible and will have the obligation to classify and categorize all Records.
- The Service Desk Manager will be consulted if there are doubts or uncertainties regarding the Classification or Categorization of Records.
- The Service Desk Analyst will inform the End User/IT Employee of the next steps to be taken.

Incident Prioritization

- The Service Desk Analyst will be responsible and will have the obligation to prioritize all Records.
- The Service Desk Manager will be consulted if there are any questions or uncertainties regarding the Priority of Records and will be informed immediately of all Incident Records prioritized as "Priority 1" and "Priority 2".
- The Incident Analyst role will be consulted when there is uncertainty regarding Service Desk Priority.

- The End User/IT Employee will be consulted regarding the Impact and Urgency of the Incident and will be informed of the next steps to be taken.

Incident attribution

The initial assignment of Incidents will be carried out using all tools, skills and techniques available at the Service Desk. This may include matching with similar Incident Records, identifying Known Errors and Workarounds, and utilizing knowledge bases

- The Service Desk Analyst will be responsible and responsible for carrying out the initial assignment of all Incident Records, with the objective of a First Contact Resolution (FCR).

- The End User/IT Employee will be consulted and informed by the Service Desk analyst as necessary and on the next steps to be taken.

Initial Incident Diagnosis

The initial diagnosis will be carried out using all the tools, skills and techniques made available by the Service Desk. This may include matching with similar Incident Records, matching with Known Errors and Workarounds, and using knowledge bases and Frequently Asked Questions (FAQ) documents.

- The Service Desk Analyst will be responsible and obliged to perform the initial diagnosis of all Incident Records with the objective of achieving First Contact Resolution (FCR).

- The End User/IT Employee will be consulted and informed by the Service Desk analyst as necessary and on the next steps to be taken.

SLA management and N2/N3 escalation

- The Service Desk Analyst will be responsible for and will have the obligation to functionally escalate the Incident to the appropriate Level 2 or Level 3 support role(s) when the Service Desk Analyst is unable to achieve First Time Resolution Problem contact within the deadlines specified in the SLA and support OLAs/UCs.
- All Level 2 or Level 3 support roles related to the Incident will be informed of the need for functional escalation and consulted for status details related to Incident resolution.
- The Incident Analyst role will be consulted when there is uncertainty surrounding the functional escalation of an Incident.
- The End User/IT Employee will be kept informed of all status changes in the reported Incident Log.

All Major Incidents will be escalated to the Service Desk management level and handled with the utmost urgency.

- The Incident Manager will be Informed, Responsible, and the Final Respondent is consulted when a Major Incident is detected.
- The Service Desk Analyst will be Responsible for immediately escalating all Major Incidents to the Service Desk Manager and will be informed of the next steps to be taken.
- The Service Desk Manager is Responsible, Consults and Informed of all Major Incidents detected, and to confirm the decision to elevate a Major Incident and contact the Incident Manager.
- Incidents prioritized as Major Incidents trigger and are handled through the Major Incident Procedure.
- The End User/IT Employee is informed of the next steps to be taken.

Investigation and Diagnosis

The Investigative and Diagnostic activity may be conducted by the Service Desk Analyst (such as Level 1 Support and First Contact Resolution) or the appropriate Level 2 or Level 3 Support group.

- The Service Desk Analyst will be responsible for ensuring that all Incidents within the Service Desk organization continue to be worked on and progressed.
- In cases where there has been no functional escalation, the Service Desk Analyst will be responsible for investigating and determining all points of failure that led to the Incident and determining the quickest solutions, which may involve a temporary solution.
- The Service Desk Analyst will be informed of any new or changed information relevant to the Incident.
- Level 2/3 Support roles will be responsible for Incidents escalated to them. They are responsible for investigating and determining all points of failure that led to the Incident and determining the quickest solutions, which may involve a temporary solution.
- Level 2/3 Support roles will be consulted for information relating to the Incident Log and will in turn be informed of any new or changed information relevant to the Incident.
- All End Users/IT Employees will be responsible for contacting the Service Desk and reporting all new symptoms and information related to the Incident, and will be informed of all significant changes in status and progress.

Necessary changes?

All resolutions for IT Hardware and Software that are NOT pre-authorized Standard Changes will be forwarded to the Change Management process in a Request for Change (RFC) and processed under Change Control.

- The Service Desk Analyst will be informed of the need to make IT Changes and is responsible for ensuring that the Change Management process is initiated for all Incidents whose resolution requires an IT Change.
- When Incident Records are assigned to the Service Desk Analyst, this role will be responsible for completing and submitting the RFC.
- When Incident Records are escalated to Level 2/3 Support, this role(s) will be responsible for informing the Service Desk Analyst of the need for an IT Change and completing and submitting the RFC.
- The Service Desk Manager is informed by the Service Desk Analyst of all changes to be made (for the purpose of raising awareness through the Service Desk to detect incoming notifications of a possible worsening of the situation).
- All End Users/IT Employees will be informed of all significant status changes and progress.

Containment and Recovery

The Resolution and Recovery activity can be performed by the Service Desk Analyst (such as Level 1 Support and First Contact Resolution) or by the appropriate group designated as Level 2 Support or Level 3 Support.

When implementing resolution and recovery plans, rollback steps should be determined whenever possible as a precaution to control the escalating Incident Impact should recovery fail or worsen the Incident.

- The Service Desk Analyst will be responsible for ensuring that all Incidents are resolved and restored to the End User/IT Employee.
    - In cases where there has been no functional escalation, the Service Desk Analyst will be responsible for determining and implementing the Incident resolution and recovery plan most likely to be successful.
    - The Service Desk Analyst will be informed of any new or changed information relevant to the Incident.

- Level 2/3 (Third Party) Support roles will be responsible for determining and implementing the Incident resolution and recovery plan most likely to be successful and reporting the results to the Service Desk Analyst.
    - Other Level 2/3 Support papers will be consulted for information related to the Incident Log.
    - Designated Level 2/3 Support roles will be kept informed of any new or changed information relevant to the Incident.

- All End Users/IT Employees will be responsible for contacting the Service Desk and reporting all new symptoms and information related to the Incident and will be consulted and informed of all significant changes in status and progress.

Incident Closure

- The Service Desk analyst will be informed of all Incident resolution activities and their results. This role is responsible and has the obligation to:
    - When the Service Desk Analyst has NOT functionally escalated the Incident, this role is responsible for providing complete documentation of the investigation, diagnosis, resolution and recovery steps taken.
    - Collect and document all information for investigation, diagnosis, resolution and recovery steps. Attaching submitted documentation is acceptable.
    - Contact and confirm the resolution of the Incident with all parties who reported the Incident.
    - Close all open Incident Records upon completion of all activities.

- The Level 2/3 Support role is responsible for informing the Service Desk of all Incident resolution activities and their results, and for presenting complete documentation of the investigation, diagnosis, resolution and recovery steps performed.
- This role is consulted for information related to Incident Closure and will be informed of the final status and closure of the Incident.

- The End User/IT Employee is available to consult information related to Incident Closure and will be informed of the final status and closure of the Incident.

Incident Prioritization Process

Severity Rating:

Description: Incidents are classified based on their severity, determined by the potential damage they can cause.
Example: Critical incidents that directly affect data integrity are treated with higher priority than those that have minimal impact.

Value of Impacted Assets:

Description: Assesses the importance of the assets involved in the incident, prioritizing those critical to the organization's operations.
Example: If an incident impacts central production servers, it may be prioritized higher than an incident that impacts less critical systems.

Risk of Spread:

Description: Considers the likelihood of the incident spreading and causing additional damage.
Example: An incident that can quickly spread across the network and compromise multiple systems can be handled with higher priority.

Impact on Business Continuity:

Description: Evaluates how the incident may affect the organization's ongoing ability to conduct business operations.
Example: Incidents that threaten to significantly disrupt business processes are given higher priority due to their critical impact.

Current External Threat:

Description: Prioritizes incidents associated with current external threats or ongoing attacks.
Example: If the organization is experiencing a real-time cyber attack, this incident can be prioritized higher for immediate response.

Historical Experience:

Description: Builds on similar incidents that have occurred previously, prioritizing based on the effectiveness of previous responses.
Example: If the organization has had success in dealing with similar incidents in the past, the previous approach can be applied for prioritization.

Legal or Regulatory Severity:

Description: Considers the severity of the incident in relation to applicable laws and regulations.
Example: Incidents that violate data protection regulations may be treated with high priority due to legal implications.

Performance metrics

The following metrics are used to monitor the performance of your organization's incident response team:

- Mean time to detection (MTTD)
- Mean time to remediation (MTTR)
- Number of incidents identified and closed in a given period
- Feedback provided by team members or customers (a qualitative indicator)
- Loss or damage caused by incidents over a certain period of time

Application

Those who violate this policy may be subject to disciplinary action, which may include termination of employment and related civil or criminal penalties.

Any supplier, consultant or contractor found to have violated this policy may be subject to sanctions that may include removal of access rights, termination of contract(s) and related civil or criminal penalties.

References

•ISO 27001, 27002, 27035
•NIST CSF: PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS-IM, RC.CO

Version

Date	Version	Description	Author