RSA Security

Incident Response Plan

By Darold Kelly, John Dyson, and Telvina Cole

Revision History

Version	Date	Author	Reason/Comments
1.00	November 12, 2023	Darold Kelly John Dyson Telvina Cole	Document Origination

RSA Technology Incident Response Plan

This confidential Incident Response Plan is developed for RSA Security (otherwise referred to as RSA) and serves as a comprehensive guide for incident management and recovery. It outlines the logical sequence of events, local incident management teams, and notification processes, emphasizing the need for quick incident recognition and effective response. The plan includes checklists, key contacts, and a clear overview of response activities. Its primary objective is to safeguard corporate assets, address incidents promptly, escalate responses as needed, and support recovery efforts. This plan aligns with RSA's commitment to people, processes, and technology in incident management and conforms to the Incident Management Policy statement detailed in the Appendix Section of the document.

Table of content

Section One – Plan Body

1. Introduction

This section serves as the initial introduction to RSA SECURITY's Incident Response Plan. The plan is designed to provide a structured and organized approach to managing and responding to incidents within RSA Security's organization. It is a confidential document, accessible only to designated members of incident management teams and individuals directly involved in the incident response and recovery processes. Each recipient of the plan is required to maintain two copies, with one stored at their office and the other at home. The plan establishes the framework for effectively recognizing and responding to incidents, swiftly assessing their nature and scope, (Mikkelsplass, 2023) and ensuring appropriate notifications are made. It emphasizes the importance of organizing response activities, including the activation of a command center when necessary, and escalating response efforts based on the severity of the incident. Furthermore, it underscores the critical role of supporting business recovery efforts in the aftermath of incidents (Moallemi 2021). RSA's commitment to people, processes, and technology in incident management is emphasized throughout the plan, and all employees and managers are reminded of their responsibility to maintain the confidentiality of the business assets.

1.2 Plan Overview:

The Incident Management Plan provides a comprehensive framework for handling incidents within RSA Security.

1.3 Objectives:

The primary objectives of the plan are to swiftly recognize and respond to incidents, efficiently assess their impact, and ensure timely notifications.

1.4 Response Structure:

The plan outlines the structure for organizing RSA's response activities, including the potential activation of a command center.

1.5 Escalation Protocol:

It defines procedures for escalating response efforts based on the severity of each incident.

1.6 Recovery Support:

In addition to immediate response actions, the plan highlights the importance of supporting recovery efforts necessary for restoring normal business operations.

1.7 Commitment to Principles:

RSA Security is committed to adhering to this plan, emphasizing the significance of people, processes, and technology in incident management.

1.8 Alignment with Policy:

The plan aligns with RSA's Incident Management Policy statement, ensuring consistency with the organization's strategic objectives and principles.

1.9 Scope

This section serves to delineate the boundaries and extent of applicability of RSA’s Incident Response Plan. It comprehensively defines the scope of incidents to which the plan is intended to respond. These incidents encompass a wide range, including cybersecurity breaches, physical security incidents, natural disasters, and other disruptive events (Kamara,2020). The plan is designed to be all-encompassing, applying uniformly to all RSA’s personnel, departments, and locations to ensure a standardized approach to incident response. It acknowledges the possibility of collaboration with external partners, such as

law enforcement agencies or third-party vendors, when deemed necessary to effectively address specific incidents.

1.10 Exclusions:

Exclusions:

This section of RSA's Incident Response Plan identifies and elucidates specific scenarios or incident types that are intentionally excluded from the plan's coverage. By defining these exclusions, the plan provides clarity and ensures that there is no ambiguity about the types of incidents that fall outside the plan's scope. Excluded incidents are expected to be addressed using alternative procedures or plans specifically tailored for those situations.

1.11 Planning Scenarios:

Within this section, the plan presents a series of hypothetical planning scenarios that function as templates for various incident types. These scenarios are designed to aid in formulating response strategies and procedures by offering guidance on how to address specific types of incidents (Huygh, 2018). They enable RSA Security to proactively prepare for a diverse set of incidents, ensuring that response efforts are well-informed and efficient.

1.11.1 Limited or No Access to the Building:

Limited or No Access to the Building: This subsection goes into detail about the planning scenario involving limited or no access to RSA's physical premises. It outlines the specific challenges, potential causes, and recommended response strategies associated with incidents that result in restricted or denied access to the workplace (Dumortier, 2020). This ensures that the organization is adequately prepared to address such situations, safeguarding both personnel and assets.

1.11.2 Loss of Data Communications, e.g., WAN, Routers:

Loss of Data Communications, e.g., WAN, Routers: This subsection provides an in-depth overview of the planning scenario related to the loss of data communications, including wide area network (WAN) and router failures. It outlines the potential impact on business operations, the importance of maintaining communication channels, and the steps to take to respond effectively to incidents affecting data connectivity.

1.11.3 Loss of Technology, e.g., Computer Room, Network Services:

Loss of Technology, e.g., Computer Room, Network Services: In this part of the plan, the focus is on the planning scenario involving the loss of critical technology components, such as computer rooms and network services (Sevda, 2021). It outlines response strategies to mitigate the impact of technology failures and disruptions, emphasizing the importance of swiftly restoring essential services.

1.11.4 Loss of People, e.g., Illness, Death:

This subsection addresses the planning scenario related to the potential loss of personnel due to reasons such as illness or death. It underscores the importance of continuity planning in the face of human resource challenges and provides guidelines for maintaining essential functions and support for affected individuals.

1.12 Recovery Objectives:

In this section, the plan defines the objectives that RSA Security aims to achieve during the recovery phase following an incident. It outlines the specific goals, such as restoring normal operations, recovering critical data, and ensuring minimal disruption to business activities. These objectives serve as a roadmap for the recovery process (Elradi, 2021).

1.13 Assumptions:

This section articulates the foundational assumptions that underpin the entire Incident Response Plan. It delineates the key assumptions made about RSA, its operations, and the external environment. These assumptions provide a common baseline for incident response planning and help guide the development and implementation of the plan by ensuring that all stakeholders share a common understanding of the operating context (Newmeyer, 2015).

Section Two – Incident Response and Management:

2.1 Logical Sequence of Events:

In this critical section, RSA Security defines a meticulously structured logical sequence of events as a comprehensive guide for responding to incidents. This step-by-step process ensures an effective and well-coordinated response to minimize disruption and damage. The sequence includes vital actions like prompt incident recognition, thorough assessment, immediate notification of relevant stakeholders, well-organized response activities, escalation protocols for complex situations, and unwavering support for business recovery efforts. By adhering to this logical sequence, RSA Security guarantees that all essential measures are taken promptly and in the correct order, safeguarding the organization from potential harm and enabling efficient incident resolution.

2.2 Local Incident Management Teams:

RSA Security recognizes the pivotal role of its Local Incident Management Teams in effectively managing incidents. This section introduces these teams and provides a deeper understanding of their crucial functions:

2.2.1 General Information:

Within this subsection, RSA Security offers foundational context about its Local Incident Management Teams. It underscores the teams' overarching purpose and role within the broader incident response framework, emphasizing their significance in maintaining operational continuity.

2.2.2 Team Overview:

Providing an insightful overview of these teams, this sub-section delves into their composition, highlighting key responsibilities and essential functions. RSA Security underscores the importance of these teams' structure and purpose in executing successful incident response efforts.

2.2.3 Local Incident Management Team:

RSA Security elaborates on the specific responsibilities and duties of its Local Incident Management Team in this sub-section. It provides a comprehensive account of the team's role during the response phase, emphasizing tasks such as effective coordination, thorough assessment, and clear communication to mitigate incidents.

Members:

Name of IRT Member	Role/Office
Moe Howard	Lead IR Specialist, email Expert
Curly Joe	IR Specialist, Physical
Larry Howard	IR Specialist, Sysadmin

2.2.4 Damage Assessment Team:

Focusing on the Damage Assessment Team, this sub-section highlights their pivotal role in evaluating and reporting the extent of damage caused by incidents. RSA Security recognizes the value of their assessments in making informed decisions, prioritizing response actions, and efficiently allocating resources to address the situation. (Al-Sartawi, 2019).

Members:

Name	Role/Office
Bruce Wayne	Damage Assessment lead; Physical and Hardware
Dick Grayson	Accounting

2.2.5 Regional Incident Management Team:

Introducing the Regional Incident Management Team, this subsection emphasizes their unique responsibilities in managing incidents that extend beyond the local level. RSA Security underscores the importance of regional coordination during larger-scale incidents and acknowledges the contributions of this team to a comprehensive incident response strategy.

Members:

Name	Role/Office
Marvin Martian	Global IR Lead / US SOC
Abe Smith	Deputy IR Lead / APAC SOC
Len Plumber	IR Lead / EU SOC

2.2.6 Threat Assessment Center:

The Threat Assessment Center's role is highlighted in this sub-section. RSA Security acknowledges their essential responsibilities in assessing and analyzing threats. Their intelligence contributes significantly to incident response strategies and the effective mitigation of threats to the organization's operations.

Members:

Name	Role/Office
Jim Bond	Lead, Global Theat Intel
Mata Hari	Global Threat Intel

2.3 Incident Management Team Activities:

Incident Management Team Activities: This section provides a comprehensive overview of the specific activities and actions that RSA's Incident Management Teams should undertake during incidents:

2.3.1 Local IM Team Activities:

Details about the activities conducted by the Local Incident Management Team are outlined in this sub-section. These activities, including incident assessment, resource coordination, communication, and incident documentation, are fundamental for effectively managing and mitigating incidents at the local level. They ensure immediate and coordinated response efforts are executed.

2.3.2 Regional Incident Manager Activities:

RSA Security emphasizes the role of the Regional Incident Manager in coordinating responses to incidents with regional impact (Shin 2015). Their responsibilities include overseeing regional resources, collaborating with local teams, and ensuring the implementation of effective response strategies to address broader regional incidents.

2.3.3 Regional IM Executive Activities:

The role of the Regional Incident Management Executive is highlighted in this sub-section, emphasizing their high-level responsibilities in decision-making and strategy development during incidents. They provide executive leadership and coordination, ensuring a cohesive regional response aligned with organizational objectives.

Section Three – Notification, Escalation, and Declaration

3.1 Introduction:

Within RSA's incident response plan, this section introduces the critical components of notification, escalation, and declaration. It underscores the paramount importance of these processes in promptly and efficiently addressing incidents, safeguarding the organization's operations and minimizing potential risks.

3.2 Notification Process Overview:

This subsection serves as a foundational understanding of the notification process's role in incident response within RSA Security. It emphasizes how timely and effective notifications are essential for initiating the incident response framework, ensuring that the right stakeholders are informed promptly.

3.2.1 Initial Notification:

In this detailed section, RSA Security outlines the procedures for initiating the initial notification process when an incident is detected. It specifies who should be contacted and the preferred means of communication, ensuring that the first steps in addressing an incident are clear and well-defined.

Telephone notification process:

During normal business hours, contact personnel at the following numbers in the order listed:

- Luke Skywalker – 867-5309
- 555-1111
- Pager: NA
- Text page (if available): NA
- Home telephone: NA
- Any other number the person has listed in the employee's list.

During non-business hours, contact personnel at the following numbers in the order listed until someone is reached:

- Leia Organa – 224-1234
- 555-2222
- Cellular: NA
- Pager: NA
- Text page (if available): NA
- Any other number the person has listed in the disaster recovery documentation.

Automated notification process:

When using an automated notification system during normal business hours, contact

personnel at the following numbers in the order listed:

- Global SOC (staffed 24/7): 800-RSA-5432
- Cellular: NA
- Pager: NA
- Text page (if available): NA
- Home telephone: NA
- Any other number the person has listed in the employee's list.

When using an automated notification system during non-business hours, contact personnel at the following numbers in the order listed until someone is reached:

- Global SOC (staffed 24/7): 800-RSA-5432
- Office: NA
- Cellular : NA
- Pager: NA
- Text page (if available):NA
- Any other number the person has listed in the DR documentation

3.3 Notification Process (Emergencies Only):

This segment of the plan focuses on the unique considerations and procedures for notifications during emergency situations. It distinguishes between routine incident notifications and those required during emergencies, emphasizing the need for swift and effective communication to mitigate escalating threats effectively.

3.3.1 Local IMT Notification and Notification of External Client, Vendor, and Business Partner:

Local IMT Notification and Notification of External Client, Vendor, and Business Partner: Within this subsection, RSA Security elaborates on the specific procedures for notifying the Local Incident Management Team during emergencies. Additionally, it outlines the steps for communicating with external stakeholders, including clients, vendors, and business partners. This ensures transparent and collaborative incident response efforts involving both internal and external parties.

Should an incident occur, the following call tree will be utilized at RSA.

Temporary staff				
Name	**Office phone**	**Home phone**	**Mobile/ Pager**	**Location**
Luke Skywalker	X111	555-1111	867-5309	HQ 4th floor
Leia Organa	X121	555-2222	224-1234	HQ 2nd floor
Han Solo	X131	555-3333	135-7099	HQ 2nd floor

3.4 Incident Response Assembly Locations:

RSA Security provides essential information regarding predetermined assembly locations for its incident response teams and personnel. These designated meeting points ensure organized and secure coordination of team members during incident response activities, enhancing the effectiveness of the response efforts.

Primary assembly area

Name: South Park & Rec Center
Address: 123 South Park Dr.
Address: (1 block from HQ office)
City/State/Zip: Boston, Mass, 02165

Secondary assembly area

Name: North Park Lake
Address: 4567 N. Park Dr.
Address: (3 blocks from HQ office)
City/State/Zip: Boston, Mass, 02165
Phone/Fax
Email

Tertiary assembly area

Name: Far Park Complex
Address 987 Distant Dr.
Address: (12 blocks west of HQ)
City/State/Zip: Boston, Mass, 02165
Phone/Fax
Email

3.5 Escalation Process (Emergencies Only):

In situations that require swift escalation, this part of the plan defines the criteria and conditions under which RSA's incident response efforts should escalate. It ensures that the organization is prepared to respond adequately to escalating threats, aligning resources and actions accordingly.

The process for escalating an incident at RSA Security is as follows:

Step 1: Follow local established emergency escalation and life/safety protocols. If these are not available, the first RSA Security employee to become aware of an incident should immediately report it to local management, who will escalate the information to the local Incident Management Team Leader or his/her designated alternate.

Step 2: Follow local established emergency escalation and life/safety protocols. If these are not available, the Damage Assessment Team should conduct an assessment of the situation. If the severity of the incident warrants, the IMT Leader or point of contact will inform the Regional Incident Manager, Threat Assessment Center, Business Continuity Management and RSA Security management of the situation.

Step 3: Follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of the local IMT assessment, and if the severity of the incident warrants, the Regional Incident Manager will coordinate with Regional Incident Management Team executives on the situation as soon as feasible by phone, email or teleconference.

Step 4: Follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of the assessment, and if the severity of the incident warrants, the TAC will notify designated senior management as deemed necessary to manage the situation; this can be done by phone, email, or teleconference.

Step 5: Continue to follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of local, regional and TAC discussions, a decision will be made on declaring a disaster:

a. IF a disaster IS NOT declared, the IMT Leader or Incident Manager will coordinate with other local management and Corporate Services staff to restore normal business operations accordingly.
b. IF a disaster IS declared, the IMT Leader or Incident Manager, in coordination with the BC Team, will invoke the BC-IM plan.

Step 6: IF a declaration is made, the IM point of contact will update the TAC, the Regional Incident Management Team and RSA's management as soon as possible.

3.6 Plan Authorization and Declaration:

This section addresses the authorization and declaration processes within RSA's incident response plan. It outlines the steps necessary to officially authorize the activation of the incident response plan and declare an incident. This includes identifying the individuals or authorities responsible for making these critical decisions, ensuring a clear and structured approach to incident management.

3.7 Declaration Process (Emergency Only):

Focusing on emergency situations, this subsection provides comprehensive guidance on how incidents are officially declared as emergencies within RSA Security. It details the criteria for such declarations, the process for making these declarations, and the subsequent actions to be taken, ensuring a well-defined and organized response to emergency incidents.

The disaster declaration process at RSA Security is as follows:

1. ONLY the management team in charge of RSA Security or his/her appointed alternate has the authority to declare a disaster at RSA.

2. A disaster declaration at RSA Security MUST generally meet one or more of the following criteria:

A. The incident is a major, prolonged or indefinite disruption to business as usual.

B. The incident is of sufficient magnitude (casualties/fatalities/property and/or facility damages/business disruptions, etc.) and warrants the enacting of emergency response and incident management measures to ensure continuity of operations at RSA.

C. The incident has met and/or exceeded the threshold of disaster declaration criteria for appropriate major public sector entities on a local, regional, national or international level.

D. Not declaring the incident, a "disaster" poses a direct threat to the viability of RSA Security as a business.

Section Four – Incident Response Checklists

4.1 Key Personnel Contact List:

This essential section of RSA's Incident Response Plan offers a comprehensive list of key personnel within the organization who play critical roles in incident response. The list includes their names, roles, contact information, and specific responsibilities related to incident management. It serves as a vital resource for swiftly reaching out to the appropriate individuals when an incident occurs, ensuring efficient and coordinated response efforts.

4.2 Key Vendor Contact List:

RSA Security recognizes the importance of engaging with key vendors and third-party contacts during incident response efforts. This section of the plan outlines a list of these crucial vendors, along with their contact details, services provided, and any contractual obligations or agreements that should be considered when involving them in the response. Having this information readily available facilitates effective collaboration with external partners during incident resolution.

4.3 Initial Incident Response Checklist:

In the early stages of an incident, RSA Security relies on a well-structured checklist to ensure that critical actions are taken promptly and methodically. This checklist itemizes essential steps, including incident verification, notification of relevant teams and personnel, securing affected systems, and preserving evidence. It guides RSA's initial response, contributing to a rapid and organized incident resolution process.

Incident occurs	☐
First person to observe incident at RSA Security follows local emergency procedures and notifies the local Damage Assessment Team and/or building security of incident.	☐
The local Damage Assessment Team assembles, investigates the incident using a checklist, and determines if the local Incident Management Team needs to be activated. If it is necessary, the DAT also notifies public authorities and/or dials 911.	☐
If needed, the DAT will notify and activate the local Incident Management Team. The IMT designates a point of contact (POC) for the incident. The POC launches a notification process.	☐
If life and safety are at immediate risk - the IMT Leader and his/her staff should act first to ensure their own survival as well as the survival of all staff, and then communicate when feasible.	☐
As soon as possible, the IMT POC notifies the Regional Incident Manager and the Threat Assessment Center via global SOC of the incident.	☐
The TAC establishes local incident coordination with the IMT point of contact, assesses the incident; and notifies senior management of the incident.	☐
The Regional Incident Manager notifies the Regional IM Team of the incident.	☐
TAC determines if the situation requires escalation, based on inputs from the Damage Assessment Team and IMT.	☐
Assuming the situation warrants escalation, the IMT reviews the situation, briefs the TAC and Regional Incident Manager, and initiates the disaster declaration process.	☐
If a disaster is not declared, IM POC advises TAC and Regional Incident Manager.	☐
If a disaster is declared, the local IMT 1. Notifies the TAC and Regional Incident Manager 2. Activates the Emergency Operations Center (EOC) 3. Activates the BC-IM plan	☐

4. Launches emergency response procedures	
The Regional Incident Manager consults with the TAC on the incident. Feedback from the TAC is relayed to local IM Team point of contact.	☐
All RSA's staff is notified of the incident and of operational status.	☐
The incident management and business continuity plans continue until the incident has been resolved.	☐

4.4 Local Incident Management Team Task Checklist:

This comprehensive checklist outlines the specific tasks and activities that the Local Incident Management Team should execute during an incident. It encompasses duties related to coordinating response efforts, conducting assessments, initiating team meetings, and maintaining open communication channels with external stakeholders.

Gather information about the incident from first-hand contact, available first responders, employees, and others; relays to Incident Manager.	☐
Account for all staff/guests on (and if applicable off) premises.	☐
Administer first aid and/or ensures life/safety measures as appropriate.	☐
Inform building security and the property management firm if they are not already aware of the incident: • Building security: xxx – xxx – xxxx • Property management firm: xxx – xxx – xxxx	☐
Inform security of the situation as soon as possible: • Security: xxx – xxx – xxxx	☐
Inform the Incident Manager as soon as possible: • IM Team Leader: xxx – xxx – xxxx	☐
Conduct an initial assessment of the incident's likely impact on local operations; coordinate with DAT.	☐
Disseminate information to local employees on the incident.	☐
Provide information about the incident to first responder organizations.	☐
Establish and maintain communications with Regional Incident Manager, Threat Assessment Center, and the appropriate business unit.	☐
Provide input as directed to the disaster declaration process.	☐
If disaster is declared, support the IM plan response.	☐

If a disaster is not declared, support recovery from the incident and restore operations accordingly.	☐
Support launch of Emergency Operations Center (EOC) according to IM plan.	☐
Provide ongoing review and analysis of incident(s) with dissemination of information to staff, Regional Incident Manager, and TAC as needed.	☐
Coordinate with counterparts in other regions as part of ongoing incident analysis.	☐
Coordinate with Operations Section leadership as well as third-party organizations to ensure that required resources are in place and ready for delivery to affected venue.	☐
Support Public Information Officer, Safety Officer and Liaison Officer roles.	☐
Support management of the incident and restores operations accordingly.	☐
Support post-event demobilization plan as needed.	☐
Assist IMT and Incident Manager as directed.	☐
Provide post-event report of activities.	☐

4.4.1 Local Incident Management Team Meeting:

Within the Local Incident Management Team Task Checklist, this sub-section dives into the critical process of convening team meetings. It defines the meeting's agenda, objectives, and procedures, emphasizing the importance of these meetings in ensuring effective coordination among team members during incident response.

Contact local IMT leader to ensure that the IMT has set an initial meeting and venue. Ensure that the presence of IMT members is recorded using the EXHIBIT 4 - RECOVERY TEAMS PERSONNEL ASSIGNMENT FORM found in the Recovery Forms section of this document.
Ensure that any missing IMT members, their alternates and any additional personnel are notified of the meeting. See the KEY CONTACTS section of this guide for a complete list of IMT members and alternates, and their contact information.
Obtain a current situation report from the IMT and Damage Assessment Team. Address the following key issues: 1. Type of event (fire, tornado, terrorism, power outage, telecomm outage, etc.) 2. Specific location of event, if known (building, floor, side of floor, etc.) 3. Magnitude of the event 4. Time of event 5. Suspected cause 6. Emergency/evacuation procedures status

7. Police and fire departments notified 8. Injuries and fatalities 9. Building access status (current access, near-term potential access) 10. Immediate impact to business operations 11. Potential for news media attention
Establish schedule of updates for Threat Assessment Center to monitor ongoing emergency response procedures. Commence providing TAC updates.
Ensure that a member of the local IMT documents, in chronological order, incident milestones and actions taken. This information will be used as a tool to update the IMT, TAC and/or other senior management.
If required, provide advice to local senior management whether employees should be sent home. Local senior management will develop a statement, determine method of communicating updates and communicate to employees.
Follow up to ensure that local management has decided whether or not to intercept 800# phone lines with a customized emergency voice recording.
Follow up to ensure that local management has decided to launch/not launch the emergency notification service, in addition to/in lieu of 800# service arrangements.

4.5 Local Incident Manager Task Checklist:

RSA's Local Incident Manager bears significant responsibilities during incident response. This checklist itemizes their specific tasks, including decision-making, resource allocation, communication, and collaboration with other teams and authorities. It provides a structured approach to the role, ensuring that the Local Incident Manager can effectively lead the incident response efforts.

Assumes overall leadership of all incident management activities.	☐
Receives information about the incident from IMT, first responders, employees, and others; contacts the Damage Assessment Team.	☐
Delegates the accounting for of all staff/guests on (and if applicable off) premises.	☐
Ensures that first aid is being provided; ensure that life/safety measures are being delivered.	☐
Informs local Business Continuity Management Team of situation as soon as possible: • Business Continuity Management Team : 123 – 456 – 7890	☐

In coordination with Damage Assessment Team, assesses the incident's likely impact on local operations.	☐
If assessment of the incident suggests a serious event that could adversely impact operations, advises Threat Assessment Center (TAC) as soon as possible.	☐
Provides input as directed to the disaster declaration process.	☐
Based on input from Regional Incident Manager and Threat Assessment Center, determines if/when to declare a disaster.	☐
If a disaster is declared, facilitates activation of IM plan; informs others (TAC, Regional Incident Manager); launches call notification.	☐
If a disaster is not declared, manages recovery from the incident and restore operations accordingly.	☐
Leads the launch of Emergency Operations Center according to IM plan; assumes role of Incident Manager.	☐
Leads the launch of Public Information Officer, Safety Officer and Liaison Officer.	☐
Ensures that Public Information Officer establishes regularly updated communications with Incident Manager and other units, e.g., Regional Incident Manager, as needed.	☐
Manages the incident and restores operations accordingly.	☐

4.5.1 Incident Response Recommended Actions:

Within the Local Incident Manager Task Checklist, this sub-section offers a set of recommended actions that the Local Incident Manager should consider during incident response. These actions are grounded in best practices and provide guidance for effective incident management, allowing the manager to make informed decisions and respond proactively.

Incident Management Team leader will develop recommendations for senior management on what overall response strategies should be implemented to facilitate the recovery of business operations in the most timely, efficient and cost-effective manner.
Consider information gathered in earlier incident and damage assessments including, but not limited to, the following: ▪ The area(s) affected by the disaster; ▪ Anticipated duration of incident;

▪ Availability of required employees; ▪ Any special timing issues such as relationship to month-end, quarter-end, etc.; ▪ Any special business issues (e.g., unusual business volume or backlog, unusual contractual obligations); ▪ Regulatory obligations; ▪ Salvageable equipment and supplies (as documented in the ASSESSMENT & EVALUATION FORMS); ▪ Availability of equipment and supplies at potential alternate or off-site locations; ▪ Salvageable records required for recovery activities; and ▪ Records which require intensive reconstruction activities.
Develop critical business function recovery priority lists for the following periods: ▪ 8 hours ▪ 12 hours ▪ 24 hours ▪ 72 hours or longer
Recommend to the Executive Management Team and Threat Assessment Center the location(s) where critical business functions and IT operations can be recovered based upon the following priority: ▪ Return to building ▪ Local sites ▪ Other sites ▪ Vendor location

4.5.2 Actions Following a Disaster Declaration:

This sub-section specifies the actions to be taken by the Local Incident Manager once a disaster declaration has been officially made. It includes activities related to coordinating with higher-level management, resource allocation, and following established escalation procedures, ensuring a well-structured response to significant incidents.

4.6 Local EOC Command Staff Task Checklist:

RSA's Emergency Operations Center (EOC) Command Staff plays a pivotal role in incident response. This checklist defines their tasks and responsibilities, covering aspects of incident command, resource management, communication, and coordination within the

EOC. It ensures that the EOC operates efficiently and aligns with established procedures during incident management.

IM TEAM PUBLIC INFORMATION OFFICER TASK CHECKLIST

When activated, establishes communications with organizations as indicated in incident management plan, e.g., Incident Manager, local management, Regional Incident Manager, and Threat Assessment Center.	☐
Establish regular time frames for reporting incident and recovery status to designated organizations.	☐
Process incoming messages from and external organizations, including police/fire/EMS and the media.	☐
Coordinate activities with Liaison Officer.	☐
Distribute approved messages to designated parties when directed.	☐
Assists IMT and Incident Manager as directed.	☐
Provide post-event report of activities.	☐

IM TEAM SAFETY OFFICER TASK CHECKLIST

When activated, monitor and manages physical safety conditions.	☐
Develop measures to ensure safety of personnel.	☐
Assist in the administering of first aid and/or ensure life/safety measures as needed.	☐
Monitor Emergency Operations Center (EOC) personnel for stress, etc.	☐
Assist Incident Manager as directed.	☐
Provide post-event report of activities.	☐

IM TEAM LIAISON OFFICER TASK CHECKLIST

When activated, interface with any/all public sector entities as appropriate, e.g., police, fire, EMS, OEM, government agencies.	☐
Disseminate information and messages to appropriate departments and individuals.	☐
Coordinate activities with Public Information Officer.	☐
Assist Incident Manager as directed.	☐
Provide post-event report of activities.	☐

4.7 Local EOC Operations Staff Task Checklist:

Within RSA's Incident Response Plan, this checklist specifies the responsibilities of the EOC Operations Staff during incident response. It outlines their roles in managing resources, facilitating communication, and handling logistics within the EOC. This checklist guarantees that EOC operations are conducted systematically and in accordance with established protocols.

PLANNING TEAM LEADER TASK CHECKLIST

When activated, prepare Incident Action Plan (IAP).	☐
Maintain situation and resource status.	☐
Coordinate BCM activities.	☐
Coordinate the preparation and dissemination of incident documentation.	☐
Provide location for subject matter and technical expertise.	☐
Prepare demobilization plan as needed.	☐
Assist Incident Manager as directed.	☐
Disseminate information and messages to appropriate departments and individuals.	☐
Provide post-event report of activities.	☐

LOGISTICS TEAM LEADER TASK CHECKLIST

When activated, organize and coordinates the provision of services (HR, communications, medical, food, transportation and housing) and support (supplies, facilities and ground support) to the incident.	☐
Disseminate information and messages to appropriate departments and individuals.	☐
Assist Incident Manager as directed.	☐
Provide post-event report of activities.	☐

OPERATIONS TEAM LEADER TASK CHECKLIST

When activated, direct and coordinates all tactical operations associated with the incident.	☐
Disseminate information and messages to appropriate departments and individuals.	☐
Assist Incident Manager as directed.	☐
Provide post-event report of activities.	☐

FINANCE TEAM LEADER TASK CHECKLIST

When activated, facilitate various administration and financial activities.	☐
Monitor incident costs and maintains financial records.	☐
Address insurance and workmen's compensation issues.	☐
Facilitate procurement activities, e.g., contracts.	☐
Monitor timekeeping and related activities.	☐
Disseminate information and messages to appropriate departments and individuals.	☐
Assist Incident Manager as directed.	☐
Provide post-event report of activities.	☐

4.8 Pre-Incident Preparations:

This critical section underscores the importance of preparatory actions before an incident occurs. It comprises several subsections that address various facets of pre-incident planning and readiness.

Establish regional response plans and procedures for dealing with incidents.	☐
Establish communications process for disseminating information about an incident to the RIMT.	☐
Point of contact for compiling information on incidents and reporting to TAC and senior management.	☐
Train alternate(s) assigned as backup to Regional Incident Manager.	☐

4.8.1 Actions Following an Incident and Prior to a Disaster Declaration Being Made:

This subsection outlines the actions and preparations that should be undertaken immediately after an incident is detected but before a formal disaster declaration is made. It includes activities related to initial response, assessment, and coordination, ensuring that RSA Security is well-prepared to address emerging incidents.

Gather input from the local Incident Management Team, Damage Assessment Team, and local senior management.	☐

Analyze the input and complete an initial assessment of the situation. Attempt to determine the potential for an evacuation or other activity that would negatively impact operations at the site.	☐
Forward the assessment results and any other intelligence to the Threat Assessment Center for analysis and action.	☐
Coordinate incident analysis with regional peers.	☐

4.8.3 Support for Local Incident Management Team Meeting:

Within this subsection, the plan elaborates on the support required to facilitate Local Incident Management Team meetings. It provides guidance on logistical preparations and coordination efforts, ensuring that these crucial meetings are productive and align with incident response objectives.

4.8.4 Actions During and After the Disaster:

This sub-section addresses actions to be taken both during and after a disaster incident. It encompasses activities such as resource allocation, response coordination, and continuous assessment during the disaster phase. Additionally, it outlines the necessary steps for recovery efforts and post-event evaluations, emphasizing the importance of learning from incidents to enhance future preparedness and response.

Ensure that InfoExchange xxx – xxx – xxxx is updated as follows: RSA Security Regional Incident Manager: Office: Cell: Home: RSA Security VP: Office: Cell: Home:	☐
Provide a brief situation report including: ▪ Nature of the incident (e.g., physical damage, life safety issues) ▪ Potential impact to business units ▪ Actions taken by local IMT and DAT ▪ Actions taken by local management ▪ Actions taken by employees ▪ Actions taken by others	☐

▪ Estimated time to return to normal operations	
Identify local EOC location and contact information.	☐
Continue updates on agreed-upon schedule.	☐
Follow up to ensure that RSA Security team leaders have notified their respective recovery team members. Document notifications in the EXHIBIT 1 - PERSONNEL NOTIFICATION CONTROL LOG found in the Recovery Forms section of this guide.	☐
Notify any other RSA Security contacts and third parties as deemed necessary. See the KEY CONTACTS section of this guide for contact information.	☐
Follow up to ensure that information regarding the status of the incident and the company's response to it is regularly communicated to the appropriate individuals and organizations.	☐
Be available to answer questions and provide input to other organizations as they enter the incident response/recovery process	☐
Be available to answer questions and provide input to other organizations as they enter the post-incident recovery and evaluation process.	☐

4.8.5 Post-Event Maintenance Activities:

In the aftermath of an incident, RSA Security recognizes the need for specific post-event maintenance actions. This includes activities related to system maintenance, data recovery, documentation of incident details, and a thorough examination of lessons learned. These post-event activities are instrumental in ensuring resilience and continuous improvement within the organization's incident response framework.

Assess regional incident management readiness.	☐
Maintain IM program through quarterly team training and updating of IM plan documentation and checklists.	☐

Section Five – Appendices

Index of Appendices

5.1 Incident Management Forms

4.1 Key Personnel Contact List:

- ☐ Name: _____
- ☐ Role: _____
- ☐ Contact Information: _____

4.2 Key Vendor Contact List:

- ☐ Vendor Name: _____
- ☐ Contact Person: _____
- ☐ Contact Information: _____

4.3 Initial Incident Response Checklist:

- ☐ Verify the incident.
- ☐ Notify relevant teams and personnel.
- ☐ Secure affected systems.
- ☐ Preserve evidence.

4.4 Local Incident Management Team Task Checklist:

- ☐ Coordinate response efforts.
- ☐ Conduct assessments.
- ☐ Initiate team meetings.
- ☐ Communicate with external stakeholders.

4.4.1 Local Incident Management Team Meeting:

- ☐ Set agenda.
- ☐ Define objectives.
- ☐ Follow meeting procedures.

4.5 Local Incident Manager Task Checklist:

- ☐ Make critical decisions.
- ☐ Allocate resources.
- ☐ Communicate effectively.
- ☐ Liaise with other teams and authorities.

4.5.1 Incident Response Recommended Actions:

- ☐ Follow best practices.
- ☐ Guide effective incident management.

4.5.2 Actions Following a Disaster Declaration:

- [ ] Coordinate with higher-level management.
- [ ] Allocate additional resources.
- [ ] Follow escalation procedures.

4.6 Local EOC Command Staff Task Checklist:

- [ ] Lead incident command.
- [ ] Manage resources.
- [ ] Ensure effective communication.
- [ ] Coordinate within the EOC.

4.7 Local EOC Operations Staff Task Checklist:

- [ ] Manage resources.
- [ ] Coordinate logistics.
- [ ] Maintain effective communication.

4.8 Pre-Incident Preparations:

4.8.1 Actions Following an Incident and Prior to a Disaster Declaration Being Made:

- [ ] Initial response.
- [ ] Assessment.
- [ ] Coordination.

4.8.3 Support for Local Incident Management Team Meeting:

- [ ] Logistical preparations.
- [ ] Coordination.

4.8.4 Actions During and After the Disaster:

- [ ] Resource allocation.
- [ ] Response coordination.
- [ ] Ongoing assessment.
- [ ] Recovery efforts.
- [ ] Post-event evaluations.

4.8.5 Post-Event Maintenance Activities:

- [ ] System maintenance.
- [ ] Data recovery.
- [ ] Documentation.
- [ ] Lessons learned.

4.8.6 Incidence Response Form

4.8.7 Incidence Response Framework Model

4.8.8 Logging, Alerting, and Monitoring Activities List

Incidence Response Form

Incident Report Form

Incident Date & Time: _____

Incident ID: _____

Reported By: _____

Contact Information: _____

Email: _____

Incident Type: [Select from dropdown]

- [ ] Phishing Attack
- [ ] Malware Infection
- [ ] Unauthorized Access
- [ ] Data Breach
- [ ] Other (Specify): _____

Description of Incident:

[Describe the incident in detail]

_____
_____
_____
_____
_____
_____
_____

Affected Systems/Resources:

[Specify affected systems, servers, applications, etc.]

_____
_____
_____
_____

Initial Assessment: (Please tick)

- [ ] Confirmed Incident
- [ ] Suspected Incident
- [ ] False Alarm

If other:_____

Incident Severity Level (Based on Triage):

- [ ] Critical
- [ ] High
- [ ] Medium
- [ ] Low

Incident Location (if applicable):

[Specify location, e.g., department, server room]

_____

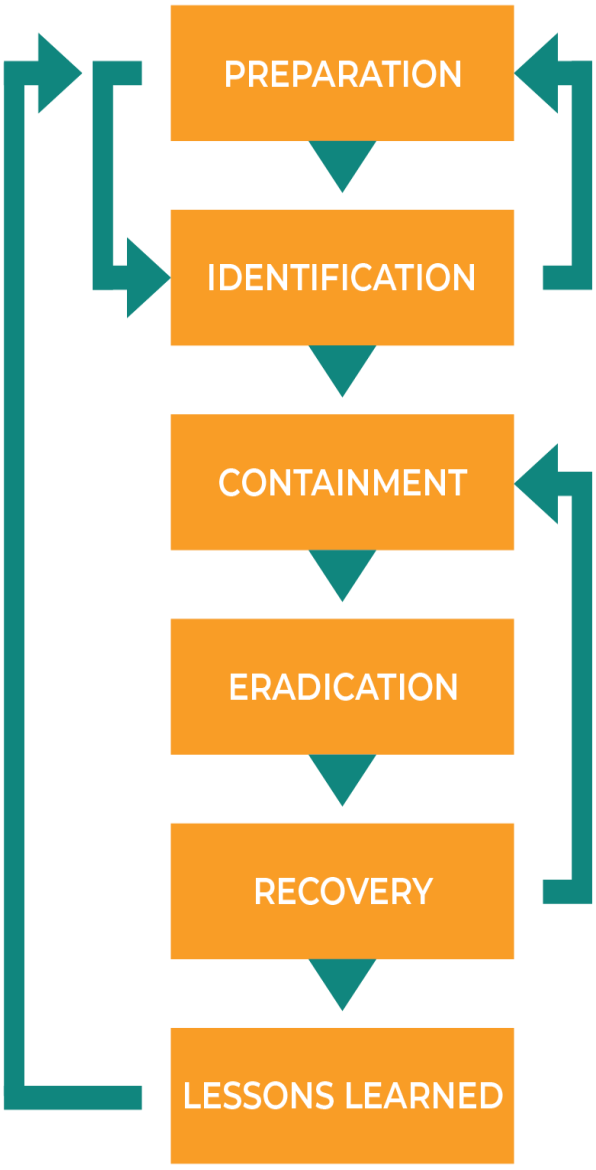
(Back of Form)

By using this IR form, RSA Security can establish a structured and effective incident response process to mitigate the impact of cybersecurity incidents and minimize potential risks to your operations and data.

Instruction

- Enter the date and time when the incident was first detected or reported.
- Assign a unique identifier to the incident for tracking purposes.
- Provide the name of the person reporting the incident.
- Include the contact details (email and phone) of the person reporting the incident for follow-up or additional information.
- Select the incident type from the dropdown list or specify it under "Other" and provide details.
- Describe the incident in detail, including how it occurred, how it was discovered, and any initial observations.
- Specify the systems, servers, applications, or resources impacted by the incident.
- Indicate whether the incident has been confirmed, is suspected, or has been identified as a false alarm.
- Assign a severity level based on predefined criteria (e.g., critical, high, medium, low).
- Provide location details if the incident is localized to a specific area or department.
- Describe immediate actions taken to contain or address the incident, such as isolating affected systems or initiating incident response procedures.
- Include any relevant additional information or comments related to the incident.

RSA's Incidence Response Framework Model



Logging, Alerting, and Monitoring Activities List

A list of logging, alerting, and monitoring activities should be kept and reviewed regularly to ensure that staff can respond to abnormal events quickly.

Prepared by:				**Date updated:**	
System/Application Name	**Logging System**	**Events Logged**	**System Owner**	**Monitoring frequency**	**Alerting**
Exchange Server	SIEM	Authentication, configuration changes, service startup/shutdown/restart	Email team	When alerts received	SOC
Webserver	SIEM	Content changes, administrator authentication	Web administrator	When alerts received	SOC
Firewall	SIEM	Rule adds/changes, blocks, success	Network team	For research	SOC
EDR	EDR console / SIEM	All actions, alerts, blocks	SOC	For research / when alerts	SOC
Network IDS	Console / SIEM	IDS Alerts	SOC	When alerts received	SOC
Server Windows Logs	SIEM	All Windows server logs	Server Team	For research	SOC

References

Al-Sartawi, A. (2019, July). Information Technology Governance: The Role of Board of Directors in Cybersecurity Oversight. In *ECCWS 2019 18th European Conference on Cyber Warfare and Security* (p. 15). Academic Conferences and publishing limited.

Dumortier, F. (2020). Security and incident reporting requirements. In *Electronic communications, audiovisual services and the internet: EU Competition Law and Regulation* (pp. 333-365). Sweet & Maxwell.

Elradi, M. D., Mohamed, M. H., & Ali, M. E. (2021). Ransomware attack: rescue-checklist cyber security awareness program. *Artificial Intelligence Advances*, *3*(1), 57-62.

Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. (2018). Answering key global IT management concerns through IT governance and management processes: A COBIT 5 View.

Kamara, I., Leenes, R., Stuurman, K., & Van den Boom, J. (2020). The cybersecurity certification landscape in the Netherlands after the Union Cybersecurity Act. *Tilburg University*.

Mikkelsplass, S. A. (2023). *Educating ICS Cybersecurity Professionals A comparative study of graduate level curricula & industry needs* (Master's thesis).

Moallemi, M., Seker, R., Mahmoud, M., Clifford, J., Pesce, J., Castro, C., ... & Klein, R. (2014). Aircraft access to system-wide information management infrastructure.

Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, *1*(3), 9-19.

Sevda, Ü. N. A. L. (2021). SİBER UZAMA YÖNELİK POLİTİK SÖYLEMDE İLETİŞİM GÜVENLİK YAKINSAMASI: ABD, AB VE TÜRKİYE ÖRNEĞİ. *Akademik Hassasiyetler*, *8*(17), 369-399.

Shin, J., Son, H., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety*, *134*, 208-217.

TechTarget (2013). Search Disaster Recovery's Incidence Response Plan. https://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/SearchDisasterRecovery_Incident_Response_Plan_Template.doc