Information Security Incident Response Procedure

v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

Document Control Information **2**
1 Introduction **4**
2 Incident Response Process Flowchart **5**
3 Incident detection and analysis **6**
3.1 Impact assessment 6
3.2 Incident prioritisation 6
4 Activating the incident response procedure **7**
5 Assemble incident response team **8**
5.1 Incident response team members 8
5.2 Roles and responsibilities 8
5.2.1 Team leader 8
5.2.2 Team facilitator 8
5.2.3 Incident liaison 9
5.2.4 Information technology 9
5.2.5 Business operations 9
5.2.6 Facilities management 9
5.2.7 Health and safety 9
5.2.8 Human resources 9
5.2.9 Business continuity planning 9
5.2.10 Communications (PR and media relations) 10
5.2.11 Legal and regulatory 10
5.3 Incident management, monitoring and communication 10
5.4 Communication procedures 10
5.4.1 External communication 11
5.4.2 Communication with the media 11
6 Incident containment, eradication, recovery and notification **12**
6.1 Containment 12
6.2 Eradication 13
6.3 Recovery 13
6.4 Notification 13
7 Post-incident activity **14**
8 Appendix A: Standard incident response team meeting agenda **15**

1 Introduction

This document is intended to be used when an incident of some kind has occurred that affects the information security of Jadarah For Dept Collections Co.. It is intended to ensure a quick, effective and orderly response to information security incidents.

The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding the actions to take.

However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this incident response procedure are to:

- Provide a concise overview of how Jadarah For Dept Collections Co. will respond to an incident affecting its information security
- Set out who will respond to an incident and their roles and responsibilities
- Describe the facilities that are in place to help with the management of the incident
- Define how decisions will be taken regarding our response to an incident
- Explain how communication within the organization and with external parties will be handled
- Provide contact details for key people and external agencies
- Define what will happen once the incident is resolved, and the responders are stood down

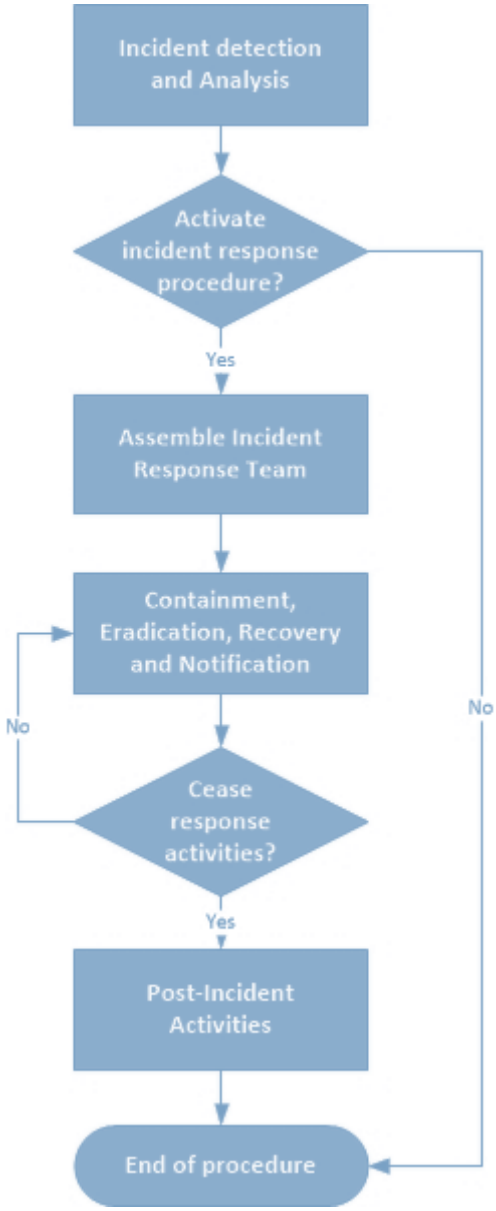
All members of staff named in this document will be given a copy which they must have available when required.

Contact details will be checked and updated at least three times a year. Changes to contact or other relevant details that occur outside of these scheduled checks should be sent to it@jadarah.sa as soon as possible after the change has occurred.

All personal information collected as part of the incident response procedure and contained in this document will be used purely for the purposes of information security incident management and is subject to relevant data protection legislation.

2 Incident Response Process Flowchart

The flow of the incident response procedure is shown in the diagram below.



These steps are explained in more detail in the rest of this procedure.

3 Incident detection and analysis

The incident may be initially detected in a wide variety of ways and through several different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within Jadarah For Dept Collections Co. or by employees noticing unusual activity (see the Information Security Event Assessment Procedure for details of how events are assessed). Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because the stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

3.1 Impact assessment

Once the incident has been detected, an initial impact assessment must be carried out (usually by the IT Support Desk) in order to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation
- The information assets that may be at risk or have been compromised
- The likely duration of the incident i.e. when it may have begun
- The business units affected and the extent of the impact to them
- Initial indication of the likely cause of the incident

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets, business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

3.2 Incident prioritisation

Based on the impact assessment, an incident will be assigned a priority of High, Medium or Low.

The guidance in the table below will be used in deciding priority.

PRIORITY	DESCRIPTION
High	Significant actual or potential disruption to the business Examples: • Malware has been detected and is spreading across the network • Unauthorised access has been detected to significant amounts of confidential data • E-Commerce website is unavailable to customers due to a possible denial of service attack
Medium	Localised disruption affecting multiple business areas Examples: • Single system unavailable • Network running slowly

	• Loss of an encrypted hard drive
Low	Localised inconvenience affecting single user Examples: • Minor breach of information security policy • Virus alert on a single computer • Sharing of password to system of lower sensitivity

As a result of this initial analysis, the IT Support Desk or any member of the management team has the authority to contact the Incident Response Team Leader at any time to ask him/her to assess whether the Information Security Incident Response Procedure should be activated. This is likely to be the case for all High priority incidents, and for Medium priority incidents where deemed appropriate.

4 Activating the incident response procedure

Once notified of an incident the Team Leader must decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response Procedure and the convening of the Incident Response Team (IRT).

An initial impact assessment will already have been made by the IT Service Desk, but further guidelines for the Team Leader regarding whether a formal incident response should be initiated for any particular incident are if any of the following apply:

- There is significant actual or potential loss of classified information
- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may cause significant impact to the organization

In the event of disagreement or uncertainty about whether to activate an incident response the decision of the Team Leader will be final.

If it is decided not to activate the procedure, then a plan should be created to allow for a lower level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.

If the incident warrants the activation of the IR procedure the Team Leader will start to assemble the IRT.

5 Assemble incident response team

Once the decision has been made to activate the incident response procedure, the Team Leader (or deputy) will ensure that all role holders (or their deputies if main role holders are un-contactable) are contacted, made aware of the nature of the incident and asked to assemble at an appropriate location.

The exception is the Incident Liaison who will be asked to attend the location of the incident (if different) in order to start to gather information for the incident assessment that the IRT will conduct so that an appropriate response can be determined.

5.1 Incident response team members

The Incident Response Team will generally consist of the following people in the roles specified and with the stated deputies, although the exact make-up of the team will vary according to the nature of the incident.

ROLE/BUSINESS AREA	MAIL ROLE HOLDER	DEPUTY
Team Leader		
Team Facilitator		
Incident Liaison		
Information Technology		
Business Operations		
Facilities Management		
Health and Safety		
Human Resources		
Business Continuity Planning		
Communications (PR and Media Relations)		
Legal and Regulatory		

Contact details for the above are listed at Appendix A of this document.

5.2 Roles and responsibilities

The responsibilities of the roles within the incident response team are as follows:

5.2.1 Team leader

- Decides whether to initiate a response
- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement

5.2.2 Team facilitator

- Supports the incident response team
- Co-ordinates resources within the command centre/war room
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status on their return to the command centre/war room
- Facilitates communication via email, fax, telephone or other methods
- Monitors external information feeds such as news

5.2.3 Incident liaison

- Attends the site of the incident as quickly as possible
- Assesses the extent and impact of the incident
- Provides first-person account of the situation to the IRT
- Liaises with the IRT on an on-going basis to provide updates and answer any questions required for decision-making by the IRT

5.2.4 Information technology

- Provides input on technology-related issues
- Assists with impact assessment

5.2.5 Business operations

- Contributes to decision-making based on knowledge of business operations, products and services
- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the organization

5.2.6 Facilities management

- Deals with aspects of physical security and access
- Provides security presence if required

5.2.7 Health and safety

- Assesses the risk to life and limb of the incident
- Ensures that legal responsibilities for health and safety are always met
- Liaises with emergency services such as police, fire and medical
- Considers environmental issues with respect to the incident

5.2.8 Human resources

- Assesses and advises on HR policy and employment contract matters
- Represents the interests of organization employees
- Advises on capability and disciplinary issues

5.2.9 Business continuity planning

- Provide advice on business continuity options
- Invoke business continuity plans if required

5.2.10 Communications (PR and media relations)

- Responsible for ensuring internal communications are effective
- Decides the level, frequency and content of communications with external parties such as the media
- Defines approach to keeping affected parties informed e.g. customers, shareholders

5.2.11 Legal and regulatory

- Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks
- Assesses the actual and potential legal implications of the incident and subsequent actions

5.3 Incident management, monitoring and communication

Once an appropriate response to the incident has been identified, the IRT needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

Regular IRT meetings must be held at an appropriate frequency decided by the Team Leader. A standard agenda for these meeting is at Appendix C. The purpose of these meetings is to ensure that incident management resources are managed effectively and that key decisions are made promptly, based on adequate information. Each meeting will be minuted by the Team Facilitator.

The Incident Liaison will provide updates to the IRT to a frequency decided by the Team Leader. These updates should be co-ordinated with the IRT meetings so that the latest information is available for each meeting.

5.4 Communication procedures

It is vital that effective communications are maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be face to face and telephone, both landline and mobile. Email should not be used unless permission to do so has been given by the IRT.

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation
- Advise internal team members of the need to refer information requests to the IRT
- If the call is answered by someone other than the contact:
- Ask if the contact is available elsewhere
- If they cannot be contacted leave a message to contact you on a given number
- Do not provide details of the Incident
- Always document call time details, responses and actions

All communications should be clearly and accurately recorded as records may be needed as part of legal action at a later date.

5.4.1 External communication

Depending on the incident there may be a variety of external parties that will be communicated with during the course of the response. It is important that the information released to third parties is managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) should be passed to the member of the IRT responsible for communications.

There may be a number of external parties who, whilst not directly involved in the incident, may be affected by it and need to be alerted to this fact. These may include:

- Customers
- Suppliers
- Shareholders
- Regulatory bodies
- Supervisory authorities

The Communications IRT member should make a list of such interested parties and define the message that is to be given to them. A list of some external agencies is given at Appendix B.

Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in a message log and passed to the Communications member of IRT.

5.4.2 Communication with the media

In general, the communication strategy with respect to the media will be to issue updates via top management. No members of staff should give an interview with the media unless this is pre-authorised by the IRT.

The preferred interface with the media will be to issue pre-written press releases. In exceptional circumstances a press conference will be held to answer questions about the incident and its effects. It is the responsibility of the Communications IRT member to arrange the venue for these and to liaise with press that may wish to attend.

In drafting a statement for the media, the following guidelines should be observed:

- Personal information should always be protected
- Stick to the facts and do not speculate about the incident or its cause
- Ensure legal advice is obtained prior to any statements being issued
- Try to pre-empt questions that may reasonably be asked
- Emphasise that a prepared response has been activated and that everything possible is being done

The following members of staff will be appointed spokespeople for the organization if further information is to be issued e.g., at a press conference:

NAME	ROLE	INCIDENT SCALE
Person A	IRT Communications	Low

Person B	Head of Corporate Communications	Medium
Person C	Chief Executive Officer	High

The most appropriate spokesperson will depend upon the scale of the incident and its effect on customers, supplier, the public and other stakeholders.

6 Incident containment, eradication, recovery and notification

6.1 Containment

The first step will be to try to stop the incident getting any worse i.e. contain it. In the case of a virus outbreak this may entail disconnecting the affected parts of the network; for a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Note: if it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions must be taken to ensure that such evidence remains admissible. This means that relevant data must not be changed either deliberately or by accident e.g. by waking up a laptop. It is recommended that specialist advice should be obtained at this point – see contacts at Appendix B.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Principle 1: Don't change any data. If anything is done that results in the data on the relevant system being altered in any way, then this will affect any subsequent court case.

Principle 2: Only access the original data in exceptional circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g., time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.

Principle 3: Always keep an audit trail of what has been done. Forensic tools will do this automatically, but this also applies to the first people on the scene. Taking photographs and videos is encouraged as long as nothing is touched to do it.

Principle 4: The person in charge must ensure that the guidelines are followed.

Prior to the arrival of a specialist basic information should be collected.

This may include:

- Photographs or videos of relevant messages or information
- Manual written records of the chronology of the incident
- Original documents, including records of who found them, where and when
- Details of any witnesses

Once collected, the evidence will be kept in a safe place where it cannot be tampered with and a formal chain of custody established.

The evidence may be required:

- For later analysis as to the cause of the incident
- As forensic evidence for criminal or civil court proceedings
- In support of any compensation negotiations with software or service suppliers

Next, a clear picture of what has happened needs to be established. The extent of the incident and the knock-on implications should be ascertained before any kind of containment action can be taken.

Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

6.2 Eradication

Actions to fix the damage caused by the incident, such as deleting malware, must be put through the change management process (as an emergency change if necessary). These actions should be aimed at fixing the current cause and preventing the incident from re-occurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

6.3 Recovery

During the recovery stage, systems should be restored back to their pre-incident condition, although necessary actions should then be performed to address any vulnerabilities that were exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers and amending procedures.

6.4 Notification

The notification of an information security incident and resulting loss of data is a sensitive issue that must be handled carefully and with full management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take. For breaches affecting personal data, see the document Personal Data Breach Notification Procedure and the template Breach Notification Letter to Data Subjects.

Jadarah For Dept Collections Co. will always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident, such as credit monitoring services.

Records collected as part of the incident response may be required as part of any resulting investigations by relevant regulatory bodies and Jadarah For Dept Collections Co. will cooperate in full with such proceedings.

7 Post-incident activity

The Team Leader will decide, based on the latest information from the Incident Liaison and other members of the team, the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of plans may continue beyond this point but under less formal management control.

This decision will be up to the Team Leader's judgement but should be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable
- The pace of change of the situation has slowed to a point where few decisions are required
- The appropriate response is well underway and recovery plans are progressing to schedule
- The degree of risk to the business has lessened to an acceptable point
- Immediate legal and regulatory responsibilities have been fulfilled

If recovery from the incident is on-going the Team Leader should define the next actions to be taken. These may include:

- Less frequent meetings of the IRT e.g. weekly depending on the circumstances
- Informing all involved parties that the IRT is standing down
- Ensuring that all documentation of the incident is secured
- Requesting that all staff not involved in further work to return to normal duties

All actions taken as part of standing down should be recorded.

After the IRT has been stood down the Team Leader will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to ensure that they reflect actual events and represent a complete and accurate record of the incident.

Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident.

8 Appendix A: Standard incident response team meeting agenda

It is recommended that the following standard agenda be used for meetings of the Incident Response Team.

AGENDA

Attendees: All members of Incident Response Team

Location: Command Centre/War Room

Frequency: Every four hours

Chair: Team Leader

Minutes: Team Facilitator

1. Actions from previous meeting
2. Incident status update
3. Decisions required
4. Task allocation
5. Internal communications
6. External communications
7. Standing down
8. Any other business