Incident Management Procedure

Reference: FPD0160A-2022

Version: 1

Owner: Lesley (new) Reeve

First Issued Date: 15/11/2023

Revision Issued Date: 15/11/2023

To outline the responsibilities and the procedures of managing an incident.

Prepared for:
All Employees, select Contractors, Partners and Customers

Prepared by:
James Pobgee

FISCAL Technologies Ltd
448 Basingstoke Road,
Reading, RG2 0LP
Tel: 0845 680 1905

FISCAL TECHNOLOGIES

1 CONFIDENTIALITY

Table of Contents

2 DOCUMENT CONTROL

Item	Description
Document Title:	Incident Management Procedure
Associated Controls:	B.5.2 B.5.24 B.5.25 B.5.26 B.5.27 B.5.28 B.5.29 B.5.37 B.6.8
Reference ID:	FPD0160A-2022
Version:	1
Status:	Published
Approver:	
Approval Date:	
First Issued Date:	10/11/2023
Revision Issued Date:	15/11/2023
Reference Documents:	Linked Policies: • Incident Management Policy Linked Procedures: Linked Records: • ISMS Scope

2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

Version	Date	Author
1	15/11/2023	James Pobgee

3 PURPOSE AND SCOPE

3.1 PURPOSE

This procedure sets out the responsibilities and the procedure of incident management to ensure an appropriate response to the detection of incidents and weaknesses of information security.

3.2 SCOPE

This process is applicable to all information and IT assets (including networks, systems, and infrastructure), information processing facilities, personnel as well as all third-party personnel within the scope of FISCAL Technologies' Information Security Management system when managing security incidents.

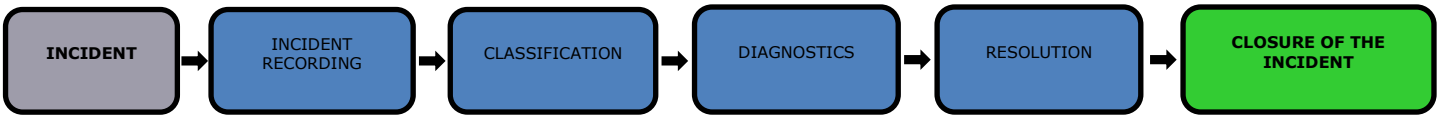
4 INCIDENT MANAGEMENT PROCEDURE

4.1 INCIDENT DISCOVERY

Incident discovery is through various inputs, including monitoring of internal or external events (including notification from system support providers of e.g., data centre systems), scheduled checks, or via telephone calls/emails.

The procedure for the management of incidents consists of the following phases:

INCIDENT MANAGEMENT PROCESS



4.2 COMMUNICATION AND INCIDENT RECORDING

- Any member of staff that has direct or indirect knowledge of any security incident, actual or suspected affecting the security of the information shall **immediately** communicate it to the Help Desk for investigation.
    - In the event that the incident is related to FISCAL's product a record must be created in Azure DevOps.
- The IT or Development team will then review the severity of the incident and escalate for classification.
- In cases where the member believes the breach to be a result of an action or negligence of the CISO / TISO, the member of staff must raise this with a member of the Executive Leadership Team and will have direct access to a member of the Executive Leadership Team throughout the incident.

4.2.1 Incidents impacting customer data.

Any incident where the security of customer data is at risk is to be notified to the customer delegate within 24 hours of discovery and with the following information:

- Categories, scope, and number of individuals/records affected.
- Time and description of the data breach including likely consequences.
- Measures already taken and proposed measures to prevent further harm.
- The name and contact details of the FISCAL person responsible for information security and / or a member of the Executive Leadership Team.

4.2.2 Example Incidents

The following are some examples of possible incidents or events, all of which are registered without exception:

- loss of service, equipment, or facilities.
- human errors.
- infringements of policies or guidelines.
- infringements of agreements of physical security.
- uncontrolled changes of the system.
- faults of software or hardware.
- access violations.
- events affecting the identification and authentication of users.
- events that affect the rights of data access.
- events affecting the procedures of backup and recovery.

Upon reporting the person should write down all details of how the incident was identified and the presumed risk and anything considered important for the resolution of the event in the description field of the incident. Under no circumstances should the user check the suspected weak points in the system except when he has the authorisation and/or supervision of the CISO, TISO or a delegate.

Whenever standard channels of communication of incidents are no longer operative, the user will contact the appropriate personnel (or Executive Leadership Team member) by message, phone and / or email until a recognition that the response has been received.

4.3 CLASSIFICATION OF THE INCIDENT

Once the incident is notified, the CISO, TISO, delegate, or a member of the Executive Leadership Team must classify it according to the security parameters that are affected and assign an appropriate priority level. The incidents can be classified into the following categories:

- Confidentiality.
- Integrity.
- Availability.
- Authentication of users.
- Related to compliance with the Data Protection Act.
- Vulnerabilities.
- Other incidents.

There are often multiple concurrent incidents, and it is therefore necessary to determine a priority level for the resolution of these.

The priority level is based on two parameters:

- **Impact**: determines the importance of the incident depending on how this affects business processes and/or the number of affected users.
- **Urgency**: depends on the maximum time delay accepted by the customer for the resolution of the incident and/or the agreed SLA.

It should also consider auxiliary factors such as the resolution time expected and the necessary resources: simple incidents will be processed as soon as possible unless this compromises the ability to allocate adequate resources to incidents with higher priority levels.

Where vulnerabilities are identified calculating the risk and priority should use the current CVSS model to identify the associated impact and urgency to resolve.

Depending on the priority, resources will be allocated as necessary to resolve the incident. The priority of the incident can change during its life cycle. For example, temporary solutions can be found that restore acceptable service levels and permit the slight delay of the closure of the incident without serious

repercussions, or mitigations may be implemented temporarily until a patch has been made available for fully eradicate the root cause.

4.3.1 Priority

The priority level will be calculated based on the following levels:

- **Critical**: any incident whose resolution permits no delay and requires immediate action due to its scope. Incidents of this type will be processed in parallel in case there are several, and in its resolution all available resources shall be utilised.
    - *Examples: Compromised IaaS platform or inability to provide customer support during office hours.*
- **High**: a high priority incident is one whose features require it to be treated before others, even if it is detected later. For this reason, an independent queue of incidents of high priority is maintained, and FISCAL will not process the lower priority incidents while there are remaining incidents in this list. High priority incidents are processed in series.
    - *Examples: high-priority incidents are considered all those where there is infiltration of a privileged account or denial of service.*
- **Medium**: by default, whilst there is no higher priority incident requiring attention, the incidents of this variety are dealt with in series in order of arrival.
    - *Examples: all incidents not classified as high priority or emergency, where the attacker has gained access to an unauthorised computer system.*
- **Low**: while there are no higher priority incidents requiring attention, low priority incidents attended to in series in order of arrival.
    - *Examples: isolated incidents on degree of attempted malicious activity, where the attacker has not achieved his purpose and it is not likely to achieve it.*

4.4 EVALUATION

Once the incident is classified, each person with responsibility for it must assess the severity of the event to decide the response actions that will be needed. It is necessary to differentiate a contingency from an incident.

Once evaluated gathered analysis and generated output shall be recorded into the associated incident within the helpdesk.

Where the incident is considered high or critical, ensure:

- Communicate and advise the CISO or TISO and the relevant Executive Leadership Team member of the incident and current priority.
- The creation of a war room within teams and include all relevant personnel, CISO, TISO and relevant Executive Leadership Team members.
    - Advise the current update on the incident and incident ID.
    - Utilise the chat room to provide regular communication on the ongoing evaluation, findings and request for additional support, resources, etc.
- The incident information is updated with the minimum information for the incident:
    - Date and time of the incident (if applicable)
    - Incident Type
    - Username of person recording the incident
    - Notes, with information provided by the person who notifies the incident.
    - Notes, with the information provided by the person who notifies the incident and could provide data or evidence of how to solve it.

If FISCAL critical activities are endangered, assess the situation in response to potential victims, material damage, services that are ceased, and activate the contingency plans. (At this stage, management procedures of business continuity should be invoked).

4.5 SCALING

When the investigating person is unable to resolve an incident in the first instance and require additional assistance of an expert or person who can make decisions that are outside of the scope of their responsibility to resolve the incident, the incident is scaled.

Scaling needs to establish some criteria within the technical support area according to the system or environment of information that set the actions to be carried out, depending on the case. There are two types of scaling:

- **Functional Scaling**: requires the support of a specialist of the highest expertise to resolve the incident.
- **Hierarchical Scaling**: refer to a higher authority responsible for making decisions that are beyond the powers assigned to that level as, for example, to allocate more resources for the resolution of a specific incident.

In case FISCAL has to divert an incident to a third party, this will also be registered in the incident management system, indicating the external company that provides the service and the service level agreed with it.

The information obtained from the evaluation of the security incidents of the information must be used to identify recurrent incidents or those with a wide scope.

The security incidents registered are reviewed by the appropriate member of Security. The review generates a report, where the various incidents detected can be seen, their classification, recurrence, and their scope with respect to the ISMS.

If registered incidents recur within a short period of time or affect the security of the system information, the established controls and procedures shall be reviewed to establish safety policies and objectives.

4.6 ANALYSIS, RESOLUTION AND CLOSURE OF INCIDENTS

In the first instance examine the incident with the aid of data recorded in the Helpdesk to determine if it can be identified with any incident already resolved, and where this is the case apply the same 'fix' as used with success previously.

If the resolution of the incident is beyond the possibilities of the Technical Area, redirect to a higher authorisation level for investigation by the assigned experts. If these experts are not able to resolve the incident, they shall follow the protocols of default scaling.

Throughout the life cycle of the incident the stored information in the Helpdesk should be updated so that stakeholders have up-to-date information on its status.

Following analysis of the incident, the ISM (or the person designated to resolve the incident) will decide what actions to perform to manage the impact, indicating, if necessary, the person responsible for execution of each corrective action.

The person responsible for managing the incident must record the following information:

- The date of the last back-up of the information and the identity of any information that was not backed-up.
- Required actions for the resolution of the incident.
- Estimated range needed for their resolution.
- Planning actions to be taken.
- People to notify in relationship to the resolution of the incident.

Prior to the resolution of security incidents that could constitute a crime, a report must be made to the FISCAL ISM (or Executive Leadership Team Member), in order to consider, the requirement for collection

of appropriate, legally viable evidence which may not be identified should the incident be reported at a later stage.

4.7 INCIDENT CLOSURE

Once the incident is settled, it is necessary to notify its closure to the user that reported the incident (and to the client, where applicable) and to indicate the date and time resolution in the incident management systems. The following information must be added to the incident record:

- Incident Number.
- Date and closing time of the incident.
- User notified of the closure.
- Comments, in which the comments made by the user and suggestions/complaints made in relation to the effectiveness of the method used to resolve the incident are recorded.
- Causation/root cause of incident (i.e., the problem), following incident investigation. Problem causation will not be known until investigation of individual contributing incidents has been conducted.

In cases in which the incident could result in an infringement of information security with legal consequences, the incident should be assessed in terms of the need to undertake the legal action deemed appropriate.

If the severity of some of the situations requires it, an extraordinary meeting of the Information Security Management System (ISMS) Board may be convened where the adoption of preventive or corrective actions of a considerable impact on the entity itself can be considered and approved via the Executive Leadership Team.

Documentation relating to incident management is retained for a minimum of a two-year period. The Helpdesk shall be reviewed on at least a quarterly basis, and findings reported to the Management Review Meeting for discussion of IT Security improvement measures.

4.8 LEARNING FROM INCIDENTS

All information security incidents will be subject to investigation. The aim being to identify and fix the root cause. The CISO, TISO or delegate will ensure that such investigations are carried out and recorded along with details of proposed corrective actions. Where necessary Information Security Management controls will be reviewed and enhanced post incident investigation and if necessary, retraining will be arranged.

During the investigation there may be a requirement to gather and retain evidence. In some cases, this evidence may be used in later disciplinary processes or legal proceedings. In such cases the CISO, TISO or other member of management will consult with the organisation's HR and legal advisers to ensure that evidence gathering is being carried out in accordance with relevant laws and regulations.

All such evidence will be retained securely until required by a member of the Executive Leadership Team or the organisation's legal advisers.