Incident Management Policy

1. Purpose

This policy details the requirements and arrangements for the reporting of all information security events and weaknesses associated with information handling facilities and information systems. It is designed to ensure that all relevant information is communicated correctly so that timely corrective action can be taken.

2. Scope

This policy applies to all Adoric Technologies LTD (or Adoric) employee.

3. Policy Definitions

3.1. Reporting Incidents

All information security events should be reported to the Founder as soon as possible following the event or incident.
The reporting procedure for all information security related events will include:
the correct actions to be taken in case of an information security event,

- noting all important details (e.g. type of non-compliance or breach, system malfunction details, screen messages, details of unusual behavior) immediately,
- not taking any action to resolve the issue prior to reporting it and obtaining advice,
- feedback mechanisms to ensure that employees are notified that the issue they have reported has been investigated and acted upon,
- reporting forms or mechanisms to assist the employee with recording and reporting all the necessary detail,
- reference to Adoric disciplinary process for dealing with users who commit or cause security breaches.

All employees should be aware that the earlier an actual or suspected security related incident is reported the more effectively it can be dealt with. Delay or failure to report an incident will often have greater repercussions for both any users involved and the organization.
Common examples of information security events and incidents are:

- loss of data, equipment, service or facilities,
- system malfunctions or overloads,
- human errors,
- non-compliance with policies, procedures or guidelines,
- breaches of physical security arrangements,
- uncontrolled system changes,
- malfunction of software or hardware – these, or other anomalous system behavior, may be an indicator of a security attack or actual breach and should always be reported and investigated,
- access control violations.

3.2. Reporting Security Weaknesses

Security weakness may be observed by any employee, whilst they may not represent an incident they should be reported for further investigation and remedial action as necessary. They should be reported to the Founder as soon as possible to prevent an incident occurring. Employees should not attempt to prove that an observed system weakness can be exploited. Testing system weaknesses could be interpreted as potential misuse of the system and may cause an information security incident to occur.

3.3. Management of Information Security Incidents and Improvements

A consistent and effective approach to the management of security incidents will be adopted by Adoric. The supporting processes will ensure that all actual or suspected information security incidents and weaknesses are handled consistently. The process for handling these will be subject to continuous improvement and will be applied to monitoring, recording, evaluating and the overall management of incidents and events. The handling of all incidents, weaknesses and security related events will consider the requirement, where necessary, to collect and preserve evidence to ensure compliance with any applicable legal requirements.

3.4. Responsibilities and Procedures

In addition to, and in support of the individual reporting responsibilities of this policy, system monitoring, alerting and vulnerability checking will be carried out. This will be used to detect potential and actual security incidents which will be subject to further investigation.
The detailed procedure for information security incident management will take account of the following guidelines:

- the procedures will be designed to handle different types of information security incidents, including:
    - information system failures and loss of service,
    - malicious code,
    - denial of service,
    - errors resulting from incomplete or inaccurate data,
    - breaches of confidentiality and integrity,
    - misuse of information systems,
- the procedures should also cover:
    - analysis and identification of the cause of the incident,
    - containment,
    - planning and implementation of corrective actions to prevent recurrence,
    - communication to all necessary parties involved with the recovery from the incident,
    - reporting the incident and mitigation plans and actions to the necessary authority,
- the collection and secure storage of audit trails and other required evidence for:
    - internal analysis,
    - retention as evidence in relation to legal of regulatory requirements where the incident may incur liability for the organization or individuals
    - negotiation of compensation from a third-party supplier of software, hardware or services,
- Actions taken to recover from security incidents and breaches should be carefully and formally controlled to ensure that:

- only nominated, authorized personnel are allowed access to live systems and data,
- all incident recovery actions are fully documented and retained,
- all emergency actions taken are reported to management for review,
- the integrity of systems, controls and data is confirmed as soon as possible.

All procedures and objectives of information security incident management should be reviewed by Founder. It should be ensured that those employees with responsibility of information security incident management understand the priorities and policy. This will include reporting responsibilities and the arrangements for handling incidents which involve other organizations and service providers.

3.5. Learning from information security incidents

Information about security incidents should be recorded and collated to enable analysis of the types, volumes, costs and root causes to take place. This information should be used to provide the basis of required improvement plans with the aim of reducing the likelihood of future recurrences. The information will also be considered when updating and revising the security policy documents.

3.6. Collection of Evidence

There are 2 primary categories of incident where the collection and preservation of evidence may be required. These are:

- Where internal HR disciplinary processes may be invoked or,
- Where the incident may lead to civil or criminal proceedings against Adoric or an individual.

When an incident is first reported the details may be incomplete or unclear. It will not usually be obvious whether there are any legal or internal disciplinary implications. Consideration should be given in every investigation to the collection and preservation of original copies of any documents, material or IT hardware which may later be required as evidence. The preservation of IT system-based evidence is complex and technical; it is unlikely that this could be effectively carried out by Adoric personnel. Any evidence used in legal proceedings must comply with detailed rules and procedures which cover:

- admissibility of evidence - whether it can be used in court,
- weight of evidence - concerning its completeness and quality,
- integrity of evidence - whether it may have been changed during or after collection.

During any investigation if it becomes apparent that the matter could lead to legal proceedings, consideration should be given to requesting the assistance of the IT service provider specialists.

4. Policy Compliance

Compliance Measurement

Founder will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, log monitoring, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

Exceptions

Any exception to the policy must be approved by Founder.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.