IDVerifact

Security Incidents Management

Produced on	May 14, 2018
Accepted/Updated on	April 7, 2021
Implementation and review supervisor	George Colwell

Document history			
No.	Date	Task	Comments
1	May 2018	Version 1.0	First Version
2	April 2019	Version 2.0	Format Update
3	April 2020	Version 2.1	Minor Updates
4	April 2021	Version 2.2	Minor Updates

Last review	April 7, 2021
Next review	April 2022

Policy Statement

IDVerifact will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the IDVerifact.

Purpose

The aim of this policy is to ensure that IDVerifact reacts appropriately to any actual or suspected security incidents relating to information systems and data.

Scope

This document applies to all IDVerifact Employees and contractual third parties who use IDVerifact IT facilities and equipment or have access to, or custody of, customer information or IDVerifact information.

All users **must** understand and adopt the use of this policy and are responsible for ensuring the safety and security of the IDVerifact's systems and the information that they use or manipulate.

Definition

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an event that is likely to lead to a security incident.

A security incident is a single event or serious of events that have caused or have the potential to cause damage to an organization's assets, reputation and/or personnel.

Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- a violation of IDVerifact computer security policies and standards
- unauthorized computer access
- loss of information confidentiality
- loss of information availability

- computer/device theft
- compromise of information integrity
- a denial-of-service condition against data, network, or computer
- misuse of service, systems, or information
- physical or logical damage to systems

Examples of security incidents include but are not limited to:

- lost or stolen equipment (computers and laptops, portable electronic devices, electronic media, paper files)
- presence of a virus or spyware or any other malicious program, including alerts from your antivirus software that your computer may have malware
- the sudden appearance of unexpected/unusual programs
- posting of confidential/restricted data to a publicly accessible web site
- inadvertent sending of restricted data to unauthorized recipients (ex. sending a sensitive e-mail to 'all staff' by mistake)
- giving information to someone who should not have access to it - verbally, in writing or electronically
- printing or copying confidential information and not storing it correctly or confidentially
- finding data that has been changed by an unauthorized person
- establishment of an unauthorized account for a computer or application
- accessing a computer using someone else's authorization (e.g. someone else's user id and password)
- unusual network connections to a computer
- sharing/revealing passwords
- unknown people asking for information which could gain them access to IDVerifact data (e.g. a password or details of a third party)
- missing "patches" and updates
- improperly configured or risky software
- use of unapproved or unlicensed software on IDVerifact equipment
- insecure disposal & re-use of equipment
- contractor / freelancers computer compromised
- development server compromised

Procedure for Incident Handling

1. Employee, vendor, customer, partner, device or sensor reports event to CISO. (email or phone)
2. CISO takes action to reduce fallout of incident – For security measures the delegation of the following but not limited to: disconnection from the network, securing evidence, blocking accounts and accesses
3. The team assigned by the CISO carries out the gathering of evidence for the purposes of:
    a. conduct internal analysis
    b. identify the cause of the incident
    c. use in the hearing of evidence
    d. negotiations of compensation from the manufacturers of software, hardware and services

   e. evaluation of compliance with the law
   f. taking legal action

4. The assigned team carries out corrective actions - planning and implementation
5. Assigned team restores systems to work after the incident, with particular emphasis on the topics: a. access control to data and systems
   b. detailed documentation of actions taken
   c. emergency actions are reported to management
6. The person responsible for customer contacts informs parties affected by the incident and provides them with all necessary information
7. Management takes, if necessary, disciplinary actions against employees responsible for the occurrence of the incident
8. All involved people carry out a detailed reporting of its activities
9. All involved people are responsible for documenting the course of the incident and restoring operations

Learning from Information Security Incidents

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by the CISO in case any patterns or trends are identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

Policy Compliance

Non-compliance with this policy could have a significant effect on the efficient operation of the IDVerifact and may result in financial loss and an inability to provide necessary services to our customers.

If any employee is found to have breached this policy, they may be subject to IDVerifact's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from HR representative or your manager.