INDEX

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Review	All	C.Santos	12/08/2024	R.Soares	21/11/2024

Summary

The management of security incidents described in this policy requires ADDVOLT to have clear guidance, policies, and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide guidance

1. Scope

This policy applies to all ADDVOLT Employees and external workers that work in ADDVOLT facilities with ADDVOLT information.

2. References, Definitions and Terminologies

None.

3. Objectives

ADDVOLT is responsible for the security and integrity of all data it holds. It must protect this data using all means necessary by always ensuring that any incident which could cause damage to ADDVOLT's assets and reputation is prevented and/or minimized.

There are many types of incidents which could affect security:

- A computer security incident is an event which could include but is not limited to:
    - Loss of confidentiality of information
    - Compromise of integrity of information
    - Denial of service
    - Unauthorized access to systems
    - Misuse of systems or information
    - Theft and damage to systems
    - Virus attacks
    - Intrusion by humans

- Other types of incidents may include:
    - Missing correspondence
    - Exposure of uncollected printouts
    - Misplaced or missing media
    - Inadvertently relaying passwords
    - Loss of mobile phones and portable devices

Ensuring efficient reporting and management of security incidents will help reduce and, in many cases, prevent further incidents from occurring.

4. General Rules

ADDVOLT has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting, and recording of security incidents. By continually updating and informing all parties identified within the scope of this policy of the importance of the identification, reporting and action required to address incidents, ADDVOLT can continue to be pro-active in addressing these incidents as and when they occur.

The types of incidents which this policy addresses include but is not limited to:

4.1. Computers left unlocked when unattended

Users of ADDVOLT computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All parties identified within the scope of this policy need to ensure they lock their computers appropriately.

4.2. Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorization. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently, or accidentally, the IT Department must be notified through ADDVOLT's Incident Reporting procedures. For more information, ADDVOLT Password policy is defined and available. Under no circumstances should an employee allow another employee to use their user account details – even under supervision.

4.3. Virus warnings/alerts

All computers in use across ADDVOLT have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft, or damage to ADDVOLT data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to the IT Department as soon as possible.

4.4. Media loss

Use of portable media such as USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets, and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorized access. Any authorized user of a portable device (including portable media) who has misplaced or suspects damage, theft whether intentional or accidental must report it immediately through ADDVOLT Incident Reporting procedures.

4.5. Data loss/disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorized - recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on ADDVOLT's website and identified as inaccurate or inappropriate
- Conversationally – information disclosed during conversation
- Press or media – unauthorized disclosure by employees or an ill-advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected printouts from Multi-Function Devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All parties identified within this policy's scope must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of ADDVOLT data.

Any loss of data and/or disclosure, whether intentional or accidental, must be reported immediately using ADDVOLT's Incident Reporting procedures.

4.6. Personal information mishandles

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc… must not be disclosed, discussed, or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.
Any abuse/misuse of such person identifiable information must be reported through ADDVOLT's Incident Reporting procedures.

4.7. Physical Security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed, or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower / floor level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data.

Continuing emphasis and re-enforcement of ADDVOLT's Clean Desk policy will further help to reduce the number of security incidents.

4.8. Logical Security / Access Controls

Controlling, managing, and restricting access to ADDVOLT's network, databases and applications is an essential part of Information Security. It is necessary to ensure only authorized employees can access information processed and maintained electronically.

4.9. Found correspondence/media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through ADDVOLT's Incident Reporting procedures.

4.10.Loss or theft of IT/information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc… or which is known/or suspected to have been stolen needs to be reported immediately through ADDVOLT's Incident Reporting procedures.

5. Responsibilities

It is the responsibility of all parties identified within the scope of this policy who undertake work for ADDVOLT, on or off the premises, to be proactive in the reporting of security incidents. ADDVOLT's Incident Reporting procedures are in place to prevent and minimize the risk of damage to the integrity and security of ADDVOLT data and information.

It is also the responsibility of all parties identified within this policy's scope to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

6. Breaches of Policy

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to ADDVOLT assets, including IT equipment and information, or conduct which is in breach of ADDVOLT's security procedures and policies.

All parties identified within the scope of this policy have a responsibility to report security incidents and breaches of this policy as quickly as possible through ADDVOLT's Incident Reporting Procedure. This obligation also extends to any external ADDVOLT contracted to support or access the Information Systems of ADDVOLT. In the case of suppliers, service providers, consultants or contractors, noncompliance could result in the immediate removal of access to the system.