INDEX

SUMMARY 1

1. SCOPE 1

2. REFERENCES, DEFINITIONS AND TERMINOLOGIES 2

3. GENERAL RULES 2

4. MONITORING AND COMPLIANCE 4

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Review	All	C.Santos	18/09/2024	Ricardo Soares	11/21/2024

Summary

ADDVOLT has a duty to ensure that all information and data which it is responsible for is securely and routinely backed up. ADDVOLT has a responsibility to ensure that information and data which has been backed up can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances.

The purpose of this policy is to identify and establish processes, procedures, and good working practices for the backup and timely recovery of ADDVOLT's information and data existing in both electronic and physical form.

1. Scope

This policy applies to the disposal of information storage media, such as those listed below, although not exclusively:

- Hard disks and backup tapes, regardless of their technology
- Hard disks of personal computers, servers and other equipment, regardless of their technology
- Paper records
- External disks or pen drives, regardless of their technology
- Mobile phones

2. References, Definitions and Terminologies

None.

3. General Rules

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data, and systems, despite the implementation of best practice. The following steps will help ensure ADDVOLT's information and data is backed up and restored securely in the most efficient manner possible:

IT Systems/Data Backups

1. ADDVOLT's IT administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed in line with Standards and Clients requirements, ADDVOLT's Disaster Recovery Procedures and departmental data retention policies.
2. All IT backup and recovery procedures must be documented, regularly reviewed, and made available to trained personnel who are responsible for performing data and IT system backup and recovery
3. All data, operating systems/domain infrastructure state data and supporting system configuration files must be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration
4. Wherever practicable backup media (e.g. External Hard Drive) must be encrypted and appropriately labeled. Any system used to manage backed-up media should enable storage of dates and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should always be kept securely with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster
5. A recording mechanism must be in place and maintained to record all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc...) including any failures or other issues relating to the backup job
6. Access to the on-site backup location and storage safe must be restricted and limited to authorized personnel only
7. Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by ADDVOLT's IT systems. Where this may not be possible, photocopies of paper files must be made and stored in a secure storage location
8. Regular tests must be carried out to establish the effectiveness of ADDVOLT's backup and restore procedures by restoring data/software from backup copies and analyzing the results. IT managers should be provided with information relating to any issues with the backup testing of their data

User Responsibilities

IT Users also have a responsibility to ensure ADDVOLT data is securely maintained and is available for backup:

1. IT Users must not store any data/files relevant to the business on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorized software which require the 'caching' of files locally in order to function). Instead, Users must save data (files) on their allocated areas – this could be a mapped drive or network shared folder the User has access to. Data (files) which are stored "locally" will NOT be backed up and will therefore be at risk of exposure, damage, corruption, or loss. The use of personal cloud systems is also included in the list of places where ADDVOLT is not to be held responsible if data becomes damaged, corrupted, or lost
2. If ADDVOLT network becomes unavailable for whatever reason and work-related data is at risk of being lost, users have no option but to save the data (files) locally (i.e. on the computer being used). Once the Corporate Network becomes available again, data (files) should be immediately transferred to the corporate network in order for it to be backed up safely and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored

Data Restores

ADDVOLT has well established backup and restore routines in place. Data (file) restores are normally carried out by the IT Team who will endeavor to restore files from a date specified by the user or from the nearest backed up date

1. Users must request data (files) to be restored by contacting the IT Department, preferably by open a ticket in the Help Desk online facility. Only files which the user is authorized to access will be provided from the restore
2. The IT Team will need to verify that the User has permission and/or authorization to view or obtain restored copies of file/s and/or folder/s. Content will be restored to the same source folder or the same area, so any requestor will need access to that folder/area to access the restored file.
3. Users requesting a restore are required to provide as much information about the data (file/s) as necessary - this will include:
    - The reason for the restore
    - The name of file/s and/or folder/s to be restored
    - Original location of file/s and/or folder/s - the Service Desk will provide guidance to the User on how to find this out
    - Date, day or time of deletion/corruption or nearest approximation
    - The last date, day, or time which the User recalls the data (files) being intact and accessed/used successfully

4. All backup and recovery (restore) procedures must be documented and made available to IT personnel responsible for carrying out data (file) restores
5. Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing or other unforeseen circumstance should be made under the supervision of the IT Team via ADDVOLT's Help Desk
6. A log must be maintained to record the use of backup media whenever it has been requested and/or used from secure storage

4. Monitoring and Compliance

ADDVOLT reserves the right to periodically audit networks and systems to ensure that they are following the requirements defined in this standard.

Accordingly, the ISMS team must monitor compliance with this standard through the various methods at its disposal and considering all Information Security requirements, including, but not limited to, management reports, internal and external audits and feedback information officer, information assets or information processing resources of the ADDVOLT.

Under no circumstances is an employee or ADDVOLT interested party authorized to engage in illegal activities under national or international law using ADDVOLT resources in their possession.