Acceptable Memory Drive Usage Policy

POL-A3N-506

1.0 Overview

As a US Military contractor, we have an unbending commitment to create the securest IT environment possible. By securing our network and IT resources we strive to protect critical governmental information and prevent potential data breaches that could compromise national security and result in A3N financial loss and reputational damage.

As part of this effort, A3N's Memory Drive Usage Policy ensures that our government contracted data is safeguarded while maintained on our devices and network.

2.0 Purpose

The purpose of this policy is to define appropriate safeguarding of sensitive government contracted data (DoD/U.S Army) maintained by A3N. Through the application of this policy the intent is to reduce the potential risks of data breaches, financial losses and reputational damage.

3.0 Scope

This policy applies to all A3N employees using A3N Information Technology (IT) Resources to conduct A3N government contracted activities. All employees must abide by this policy in a way that supports the security and protection of government data.

A3n roles and responsibilities include (but not limited to):

Managers
Responsible for ensuring compliance with this procedure by the A3N employees in their department. This includes requiring training and monitoring compliance.

Employees
Responsible for safeguarding access to, and appropriate use of any IT Resources for A3N government contracted purposes.

Information Security Services (INFOSEC)
Responsible for monitoring the use of A3N IT Resources in order to safeguard A3N government contracted Information.

4.0 Definitions

In accordance with A3N standards, Removable Media Devices (RMD) are an approved IT resource when granted proper authorization through the INFOSEC.

The following are the only A3N approved RMD:

- External Hard Drives
- USB Memory Drives
- Media Cards (SD, micro-SD, etc)

5.0 Policy Definition

5.1 Acceptable Use

To reduce potential risks and to protect information this policy requires the following:

- A3N employees may only use INFOSEC approved and encrypted RMDs.
- A3N approved RMDs may not be connected to or used in Non-A3N computers.
- Sensitive information should be stored on RMDs only when:
  - Required in the performance of your assigned duties.
  - Providing required information from other state or federal agencies.
- Sensitive information stored on RMDs must:
  - Be encrypted in accordance with the A3N/DoD encryption policies.
  - Be labeled with a red coded sticker identifying the sensitive classification level.*

    * *Please refer to applicable DoD policy, AR 380-5, regarding the labeling of classified information. If unsure of what classification level the information you are storing falls into, please contact the A3N Solutions INFOSEC team.*

5.1 Disposal/Destruction

- Red coded removable RMDs that have reached EOL or have become damaged must be relinquished to INFOSEC for proper decommission, disposal and destruction.
- The INFOSEC team will abide by DoD Data wiping standards.

5.2 Incident Management

- In the event that a red coded RMD has been lost or suspected to be lost, it is the responsibility of the employee to notify his or her immediate manager and INFOSEC.
- Any misuse or irresponsible actions that affect A3N or client data must be reported as a security incident to the INFOSEC department.

6.0 Compliance

A3N INFOSEC will exercise the following measures to ensure the policy is enforced:

6.1 Monitoring

Compliance monitoring will be completed through the following (including but not limited to):

- IT System Tool & Reports
- Audits (Internal and External)
- Management Feedback
- Periodic walkthroughs

6.2 Training

As part of HR orientation, all new hires are required to complete the following training:

- POL-A3N-506 (review and acknowledge)
- Removable Media Training video

A3N Managers are accountable to ensure direct reports complete training on this policy.
Upon completion of this training a certificate is will be maintained by HR.

6.3 Exceptions

Any exception to this policy must have advanced approval from the INFOSEC team.

6.4 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including:

- Written Reprimand
- Suspension
- Termination of employment
- Federal prosecution

7.0 Administrative Policy Review

Management and the INFOSEC team will review this policy (and revise as necessary) at minimum once every 24 months. In the event a security breach has occurred a review of this and any related policies, standards, and procedures must be reviewed and revised as necessary within 30 days of the event.

8.0 Related Policies, Standards, and Procedures

- U.S. Army Information Security Program (AR 380-5)
- U.S. Army Information Assurance (AR 25-2)
- Encryption standards found in NIST Federal Information Processing Standards (FIPS)
  - 140-2(l)
  - 197(m)
  - 800-38A(n)

Date Last Reviewed	06 May 16
Date Last Revised	06 May 16