WipeDrive Compliance:
National Electronic Security Authority (NESA) in the United Arab Emirates (UAE)

www.WhiteCanyon.com | Sales@WhiteCanyon.com | 1 (801) 224-8900

Overview

The United Arab Emirates requires all agencies meet National Electronic Security Authority (NESA) compliance regulations. These regulations are meant to limit the exposure of data loss and data breaches by government agencies. This report reviews the NESA requirements and what UAE agencies can do to meet them.

The National Electronic Security Authority (NESA) is the United Arab Emirates (UAE) federal authority responsible for the innovation cybersecurity across the nation. NESA has produced the UAE Information Assurance Standards (UAE IAS), which is a set of standards and guidelines for government entities in critical sectors. These standards are to protect the UAE's critical data infrastructure and advance national cybersecurity. Compliance with these standards is mandatory for all government organizations, semi-government organizations and critical infrastructure business organizations. By complying organizations will ensure the following:

- Protection of information assets
- Compliance with UAE regulations
- Mitigation of identified information security risks
- Implementation of effective controls
- Establishment of a secure culture by raising awareness

ENFORCEMENT

UAE IAS is a set of 188 security controls and standards grouped into four different priority tiers. Organizations are expected to meet all security controls and standards. NESA will perform a Risk Assessment Framework on all organizations and will enforce compliance with the regulations. NESA has yet to outline a mandatory compliance date for organizations, or any potential fines, but these controls are required to be implemented by all the relevant entities.

THE ROLE OF WIPEDRIVE

The WipeDrive Enterprise solution will sanitize data on workstations, servers, mobile devices and all an organization's IT assets. The sanitization will ensure that all data has been securely erased to meet NESA requirements before a device leaves an organization. WipeDrive also provides hash-encrypted Audit Report for each IT asset for proof of erasure to NESA regulators.

The WipeDrive solution also provides the freedom to save Audit Reports to any location. There is no requirement for a Management Console or other systems installed on your internal networks.

The WipeDrive Enterprise, SecureClean and WipeDrive Mobile solutions allows organizations to comply with the following NESA Standards:

NESA: Management Control Family
M4.4.2: Return of Assets Priority Tier: P1
In cases where an employee, contractor, or third-party user purchases the entity's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the entity and securely erased from the equipment.
M1.4.3: Documentation Priority Tier: P2
Documents are disposed of in accordance with the procedures applicable to their classification.

NESA: Technical Control Family
T1.4.2: Disposal of Media Priority Tier: P2
CONTROL: The entity shall dispose media when no longer needed. **SUB-CONTROL:** **1.** The entity shall establish procedures for secure disposal of media containing confidential information based on the sensitivity of that information. **2.** The entity shall destroy media, both paper and digital, when no longer serving the entity. **The following items should be considered:** **1.** Media containing confidential information should be stored and disposed of securely and safely, e.g. by incineration or shredding, or erasing data for use by another application within the entity. **2.** Procedures should be in place to identify the items that might require secure disposal. **3.** It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items. **4.** Many entities offer collection and disposal services for media; care should be taken in selecting a suitable external party with adequate controls and experience. Disposal of sensitive items should be logged where possible in order to maintain an audit trail.

NESA: Technical Control Family - continued
T7.5.2: Protection of Systems Test Data Priority Tier: P3
CONTROL: The entity shall ensure the protection of system test data. **SUB-CONTROL:** : The entity shall erase any data from test applications immediately after testing is completed. Operational information should be erased from a test application system immediately after the testing is complete.
T2.3.6: Secure Disposal or Reuse of Equipment Priority Tier: P3
CONTROL: The entity shall ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. **SUB-CONTROL:** The entity shall establish procedures for secure disposal or reuse of equipment based on the sensitivity of stored information.
T1.4.1: Management of Removable Media Priority Tier: P1
The entity shall establish media management procedures along its life cycle (setup, distribution, utilization, and disposal). The following guidelines for the management of removable media should be considered: **A.** If no longer required, the contents of any re-usable media that are to be removed from the entity should be made unrecoverable; data wiping software could be used for instance. Where necessary and practical, authorization should be required for media removed from the entity and a record of such removals should be kept in order to maintain an audit trail.

Contact a WipeDrive Enterprise Sales Executive today to find out how your agency can meet NESA compliance.