Department of Commerce · National Oceanic & Atmospheric Administration · National Weather Service

NATIONAL WEATHER SERVICE EASTERN REGION SUPPLEMENT 02-2019
APPLICABLE TO NWSI 60-702
SEPTEMBER 26, 2019

Information Technology
Information Technology Security Policy, NWSPD 60-7
Management, Operational and Technical Controls, NWSI 60-702

Laptop Management Policy

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/

OPR: W/ER41 (N. Rappold) **Certified by:** W/ER4 (P. Gabrielsen)
Type of Issuance: Initial

SUMMARY OF REVISIONS: Initial issuance. Establishes policy for the use and deployment of laptops within Eastern Region (NOAA8882 FISMA System). Implements applicable management and configuration controls required by NOAA IT Security Manual (NOAA ITSM), the NOAA8882 System Security Plan (SSP), National Institute for Standards and Technology (NIST), 800-53 Revision 4 and other applicable Departmental and Presidential Directives.

Signed_____September 12, 2019____
Mickey Brown Date
Acting Director, Eastern Region

Table of Contents Page

1 Introduction

This memorandum establishes policy for the use and deployment of laptops within Eastern Region FISMA Boundary (NOAA8882), in accordance with DoC/NOAA/NWS policies.

2 Scope

This policy applies to all laptops that are configured, deployed and managed by NOAA8882 system owner. All laptops that are Eastern Region inventoried property shall be configured to adhere to this supplement.

3 Background

Eastern Region is a member of Enterprise Mission Enabling System (EMES), which provides policy, procedures and direction on a number of Enterprise solutions for security, inventory, configuration management and encryption. Specific examples are listed in Appendix A. Eastern Region secures, updates, and maintains the IT systems by utilizing Enterprise and Domain level systems in place.

4 Definitions

FISMA: Federal Information Security Management Act of 2002.
NIST: National Institute of Standards and Technology.
NIST 800-53 "Recommended Security Controls for Federal Information Systems": NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems.
NOAA Information Technology Security Manual (NOAA ITSM): The purpose of the NOAA ITSM is to define the requirements necessary for all of NOAA systems to meet the fundamental security and privacy objectives of system and data confidentiality, integrity, and availability.

5 Roles and Responsibilities

A. **System Owner (SO)**: The principal person responsible for the management and operations of all IT systems within the NOAA8882 system boundary. The System Operations Division (SOD) Chief is assigned this role.

B. **Domain Administrator (DA)**: Manages and updates the configuration baselines, provides guidance and support with Active Directory, McAfee, IBM BigFix, Encryption, and Scanning/Patching, relating to this policy.

C. **System Administrator (SA)**: Responsible for configuring and managing local NOAA8882 equipment. Must ensure equipment is configured to adhere to the policy as stated and that all equipment is properly scanned and patched on a monthly basis.

D. **User**: The user is an approved NOAA employee, contractor, or visitor with an authorized user account for using the IT system to achieve the NOAA/NWS mission. The user is responsible for providing access to any assigned government furnished equipment to the system administrator or designee in a timely manner, so the equipment can be scanned, patched and checked for compliance.

6 Process/Requirements

a. Active Directory
   i. All Windows and Linux devices must be joined to Active Directory.
   ii. User accounts on devices shall be tied to Active Directory.

b. Encryption
   i. As per NOAA ITSM:
   ii. Full-device encryption must be used to protect the confidentiality and integrity of information on all NOAA approved mobile devices.

c. Scanning/Patching
   i. As per NOAA ITSM:
   ii. All NOAA8882 IT systems are required to be scanned for vulnerabilities monthly.
   iii. Laptop patching shall be done monthly by local system administrators or designee.

d. Anti-Virus
   i. All laptops are required to have NOAA8882 approved antivirus software installed and activated, which serves as the primarily line of defense against malicious software.
   ii. Antivirus software shall be configured to scan on a weekly basis.

e. Transitioning external to internal WAN/LAN
   i. Devices will be permitted to connect to the NOAA8882 internal network without having a full scan performed.

Appendix A – Enterprise Solutions

Enterprise solutions for security, inventory, configuration management and encryption include but are not limited to; Active Directory, McAfee ePo, McAfee Endpoint Encryption for PC (EEPC), and IBM's BigFix (ECMO).

A. Active Directory
    a. All Windows and Linux devices must be joined to Active Directory.
    b. Linux devices require Centrify or equivalent NOAA8882 approved software to be installed and configured appropriately so that the device may be joined to Active Directory.
    c. User accounts on devices shall be tied to Active Directory.

B. Encryption
    a. As per NOAA ITSM:
        i. Full-device encryption must be used to protect the confidentiality and integrity of information on all NOAA approved mobile devices.
    b. McAfee Endpoint Encryption for PC is required on all NOAA8882 Windows laptop devices.

C. Anti-virus Software
    a. Windows devices are required to install McAfee ePO Antivirus software.
    b. Linux devices are required to install Clam AV.

D. IBM BigFix (ECMO)
    a. The IBM BigFix client is required on all devices, including laptops.
    b. The latest client can be downloaded from the internal or external Secure FTP servers.

E. Scanning/Patching
    a. All NOAA8882 IT systems will be scanned for vulnerabilities monthly.
    b. Laptop patching shall be done monthly by local IT system administrators.

Appendix B – Exempted Test Equipment

For a laptop to be defined as “Test Equipment” and exempted from this policy it must:

a. Run an operating system older than Windows 10.
b. Remain off the NOAA8882 network.
c. Used exclusively as an interface for a NWS observation or dissemination system (ASOS, NWR, Radar, etc.).
d. Shall not be used for tasks, such as checking email, web browsing or non-test equipment/interface tasks.
e. These devices will be limited and inventoried on the ER inventory list.
f. Any exemptions to this shall be approved by the System Owner.

Appendix C – Impact-Based Decision Support Services (IDSS) Laptops

Government Furnished Equipment (GFE) should be the only devices that are used to provide IDSS support to our customers and partners. Personal owned equipment shall not be connected to the NOAA8882 network or used to provide IDSS to customers or connected partner networks.

The local system administrator and the deployed Eastern Region employee must follow these procedures when using GFE for IDSS onsite support.

1. GFE laptops being mobilized for IDSS onsite support shall be registered on active directory; have full device encryption; have approved Anti-virus software installed and activated; have ECMO client installed and be scanned for vulnerabilities and patched monthly.

2. Before an Eastern Region employee goes on site with a GFE laptop, it is their responsibility to validate that their Common Access Card (CAC) allows them access to the system; the laptop functions correctly and all necessary software for IDSS is loaded and working. A property hand receipt is required if the system is going off site.

    a. If the GFE laptop originates from Eastern Region Headquarters (ERHQ), then ERHQ is responsible that the laptop is working properly.

3. When a deployment occurs, depending on the duration and scope, either the local system administrator or Information Systems and Services (ISS) in coordination with the Eastern Region's Regional Operations Center will be notified and provide deployment support.

4. Once the deployed employee returns to the office, it is their responsibility to return the laptop to the local system administrator and ensure the property hand receipt is cleared by the office property custodian.

5. It is the responsibility of the local system administrator to make sure the system is up-to-date according to the procedures in Appendix A.

6. It is the responsibility of the local system administrator to log the time maintaining GFE IDSS laptops in EMRS.

Appendix D – System Administration Best Practices

1. During the monthly security scan the following will be done:
    a. Make sure all software is up-to-date
    b. Perform McAfee scans
    c. Clear temp credentials and settings
    d. Cache the emergency backup accounts
    e. Ensure property documentation is current
2. Support for lost or failed CAC
    a. Local or regional SA provides temporary user name and password for McAfee endpoint encryption
    b. Local SA provides emergency AD account - preferred method
    c. If needed regional SA provides local administrator account