Northwestern
INFORMATION TECHNOLOGY

Fundamental Cybersecurity Safeguards

February 5, 2024

Why talk about this now?

ACQUISITION.GOV

FAR 52.204-21

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

What are basic safeguards?

Fundamental cyber hygiene practices and principles

Safeguards, in general, are protective measures prescribed to meet security requirements (e.g., confidentiality, availability, integrity). Safeguards include security features, management constraints, personnel security and physical security.

Northwestern has standardized on 17 minimum safeguards that align to foundational practices described in federal regulations and contracts. These safeguards cover access control, identification and authentication, media protection, physical protection, systems/communication protection, and system/information integrity.

These safeguards apply to ALL systems, processes, and personnel that store, process, or transmit federally supported research data.

Control Requirements vs Controls

Control requirements tell us what to do, but they do not do a great job of telling us how to do it.

Controls are step-by-step procedures applied to address risk

Control Requirements

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Verify and control/limit connections to and use of external information systems.	Control information posted or processed on publicly accessible information systems.	Identify information system users, processes acting on behalf of users, or devices.
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.*	Monitor, control, and protect organizational communications	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Identity, report, and correct information and information system flaws in a timely manner.
Provide protection from malicious code at appropriate locations within organizational information systems.	Update malicious code protection mechanisms when new releases are available.	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.*	Escort visitors and monitor visitor activity.*
Maintain audit logs of physical access.*	Control and manage physical access devices.*			

*Not included in current implementation guidance for NSPM-33 and apply to "servers" and not endpoints at NU

What does that mean?

These are easier to do if systems are owned and managed by Northwestern

Use passwords or PINs for all systems and devices (preferably NetIDs or other centrally-provisioned identities)

Control user rights, (role-based access control, and proper use of admin privileges)

Use secured and trusted networks, and a VPN if that's not possible (particularly international)

Limit sharing capabilities and use secure settings (e.g. password protection), even on trusted cloud systems

Don’t allow password sharing and create individual accounts for all personnel.

Change default passwords and ensure all devices mobile, desktop, etc. are all password protected.

Shred any physical documents that are no longer of use, or perform multiple data erasures before disposing or redeploying computer equipment

Ensure that firewalls block traffic from the internet by default, and that all devices and terminals fall within the boundaries of the firewall.

Individuals should not attempt to run their servers that are directly connected to the internet. Web hosting should be done through Northwestern or a hosted company with assessed security procedures.

PATCH YOUR SYSTEMS AND APPLICATIONS. Only use supported software.

Ensure that all computers have antivirus installed **with ransomware protection capabilities**, preferably Northwestern’s Advanced Threat Protection (Crowdstrike).

Ensure that the antivirus and firewalls are eligible for updates.

Enable virus scanning capabilities on antivirus software and ensure the scans are run frequently (not required for Crowdstrike)

Use NU Datacenter or Cloud services for all servers

Questions?

Brandon Grill
Senior Director, Information Security
bgrill@northwestern.edu

Paul Hinds
Security and Privacy Advisor
paul.hinds@northwestern.edu