Northgate Defense Systems, LLC	Document ID	POL-AC
	Version	1.0
Access Control Policy	Effective Date	March 1, 2026
	Document Owner	Rachel Okafor
	Approved By	David Whitfield

Table of Contents

1. Purpose

This Access Control Policy establishes requirements for managing access to information systems that store, process, or transmit Controlled Unclassified Information (CUI) at Northgate Defense Systems, LLC. Effective access control is fundamental to protecting CUI from unauthorized disclosure and ensuring compliance with CMMC Level 2 requirements.

This policy addresses the 22 access control requirements defined in NIST SP 800-171 Rev 2 (Control Family 3.1). These requirements govern who can access systems, what actions they can perform, how access is monitored, and how remote, wireless, and mobile access is secured.

Access control failures are among the most common causes of security incidents. By implementing the controls in this policy, Northgate Defense Systems, LLC reduces the risk of unauthorized access to CUI, whether from external attackers, malicious insiders, or accidental exposure.

2. Scope

2.1 Systems

This policy applies to all information systems within the CMMC assessment boundary that store, process, or transmit CUI. This includes servers and workstations in the CUI enclave, network infrastructure supporting CUI systems, cloud services processing CUI, remote access systems (VPN, remote desktop), wireless networks accessible from CUI systems, and mobile devices authorized to access CUI.

2.2 Personnel

This policy applies to all personnel with access to CUI systems, including employees, contractors, and third-party personnel with authorized access.

2.3 CUI Types

Northgate Defense Systems, LLC handles the following CUI categories: [Specify categories, e.g., CTI - Controlled Technical Information, ITAR - International Traffic in Arms Regulations data, Export Controlled information]. Access controls are applied based on the sensitivity of information and need-to-know requirements.

> **SMB Implementation Tip:** Define your CUI boundary clearly. Only systems that actually touch CUI need these controls. Keeping the boundary small reduces compliance burden.

3. Roles and Responsibilities

Role	Access Control Responsibilities

Senior Management	Approve access control policy; authorize exceptions; ensure resources for access management; review quarterly access reports
IT Manager	Approve access requests; define access roles; conduct access reviews; authorize remote/wireless/mobile access; investigate access violations
System Administrator	Provision and deprovision accounts; configure access controls on systems; implement session settings; maintain access logs; support access reviews
Data/System Owners	Define access requirements for their systems; approve access to their data; participate in access reviews
All Users	Request access through proper channels; protect credentials; use only authorized access; report suspicious activity; lock workstations when unattended

4. Policy Requirements

4.1 Account Management (3.1.1, 3.1.2)

All access to CUI systems requires an authorized user account. Accounts are provisioned based on verified business need and job function.

4.1.1 Account Types

Account Type	Purpose	Approval Required	Review Frequency
Standard User	Day-to-day business functions	IT Manager	Quarterly
Privileged/Admin	System administration, security functions	IT Manager + Senior Mgmt	Monthly
Service Account	Application-to-application communication	IT Manager	Quarterly
Contractor	Third-party personnel access	IT Manager + Sponsor	Per contract, min quarterly
Temporary	Short-term project access	IT Manager	Weekly during active use

4.1.2 Account Provisioning

New accounts require a documented access request with business justification. Requests must identify the specific systems and access level needed. Approval must be obtained before account creation. Accounts are configured with the minimum permissions required for the role. New users must acknowledge the Acceptable Use Policy before access is granted. Account provisioning is completed within 3 business days of the approved request.

4.1.3 Account Modification

Access changes due to a role change require a new access request. Previous access not required for the new role is removed within 24 hours. Lateral moves trigger a full access review before new access is provisioned.

4.1.4 Account Termination

Accounts are disabled within 24 hours of employment termination. For involuntary terminations, accounts are disabled before or concurrent with notification. Disabled accounts are deleted after 90 days unless retention is required. Upon termination, access badges, tokens, and keys are collected.

> **SMB Implementation Tip:** Create an account request form that captures: user name, role, systems needed, business justification, approver. Keep it simple but documented.

4.2 Access Enforcement (3.1.2)

Systems enforce approved access permissions. Access is restricted to authorized transactions and functions based on user role.

4.2.1 Role-Based Access Control

Northgate Defense Systems, LLC implements role-based access control (RBAC) for CUI systems. Access roles are defined based on job functions. Users are assigned to roles, not individual permissions where possible. Role definitions are documented and reviewed annually. Changes to role definitions follow change management process.

4.2.2 Access Control Implementation

File systems enforce permissions through Active Directory security groups. Applications enforce role-based permissions at the application layer. Database access is restricted to application service accounts and authorized DBAs. Network access is controlled through firewall rules and network segmentation.

4.3 Information Flow Control (3.1.3)

The flow of CUI is controlled to prevent unauthorized disclosure.

4.3.1 CUI Flow Restrictions

CUI is stored only in designated locations within the assessment boundary. CUI is not transmitted to systems outside the boundary without authorization. Email containing CUI requires encryption. File transfers containing CUI use approved secure methods. CUI is not copied to removable media without authorization and encryption.

4.3.2 Technical Controls

Data Loss Prevention (DLP) monitors for CUI leaving the boundary. Email gateway scans for CUI patterns in outbound email. USB ports are disabled or restricted on CUI workstations. Cloud storage is restricted to approved, compliant services.

4.4 Separation of Duties (3.1.4)

Duties are separated to reduce the risk of malicious or erroneous actions.

4.4.1 Required Separations

Function	Separated From	Rationale
System administration	Security log review	Admins cannot modify logs they might be subject of
Access provisioning	Access approval	Provisioner cannot self-approve access
Change implementation	Change approval	Developer cannot approve own changes to production
Backup administration	Restore execution	Prevents unauthorized data restoration
User account creation	Privileged role assignment	Prevents privilege escalation

SMB Implementation Tip: In small teams, perfect separation isn't always possible. Document compensating controls: if one person must do both functions, ensure their actions are logged and reviewed by someone else.

4.5 Least Privilege (3.1.5, 3.1.6, 3.1.7)

Users are granted only the minimum access required to perform their duties.

4.5.1 Least Privilege Principles

Access is granted based on need-to-know and job function. Default access for new accounts is no access until specifically provisioned. Access requests must justify why the requested level is necessary. Broad access (e.g., domain admin, root) is granted only when specific need is demonstrated.

4.5.2 Privileged Access Management

Privileged accounts are used only for administrative tasks. Administrators maintain separate standard accounts for email, browsing, and daily work. Privileged credentials are not used for routine activities. Privileged account usage is logged and reviewed monthly. Privileged access requires multi-factor authentication.

4.5.3 Privilege Restrictions

Parameter	Requirement
Domain Admin accounts	Maximum 3 accounts, named individuals only
Local Admin rights	Removed from standard users; IT staff only
Root/sudo access	Limited to designated system administrators
Database admin access	Limited to DBA role; application uses limited service accounts
Security tool admin	Separate from system administrators where feasible

4.6 Unsuccessful Logon Attempts (3.1.8)

Systems limit unsuccessful logon attempts to prevent brute force attacks.

4.6.1 Lockout Parameters

Parameter	Setting	Rationale

Failed attempts before lockout	5 attempts	Balance security with usability
Lockout duration	30 minutes minimum	Auto-unlock after timeout
Failed attempt counter reset	30 minutes	Counter resets after period without failures
Admin unlock	Available	IT can unlock before timeout if verified

4.6.2 Lockout Monitoring

Account lockouts are logged with timestamp, username, and source. Multiple lockouts from the same source trigger an investigation. Patterns suggesting an attack (multiple accounts, rapid attempts) are escalated to incident response.

4.7 System Use Notification (3.1.9)

Systems display approved use notification before granting access.

4.7.1 Login Banner Requirements

All CUI systems display a login banner before authentication. The banner includes notice that the system is for authorized use only, that use may be monitored and recorded, that unauthorized use is prohibited and subject to criminal/civil penalties, and a consent statement that use constitutes consent to monitoring.

4.7.2 Banner Text

Standard banner text: 'This system is the property of Northgate Defense Systems, LLC and is for authorized use only. By using this system, you consent to monitoring and recording. Unauthorized use is prohibited and may result in disciplinary action and/or criminal prosecution. If you are not authorized to use this system, disconnect now.'

4.8 Session Controls (3.1.10, 3.1.11)

User sessions are managed to prevent unauthorized access to unattended systems.

4.8.1 Session Lock

Control	Requirement
Inactivity timeout	15 minutes maximum
Lock behavior	Requires re-authentication to unlock
Screen display	Pattern-hiding (blank screen or screensaver, no data visible)
Manual lock	Users must lock workstation when leaving desk (Windows+L)

4.8.2 Session Termination

Sessions terminate automatically after defined conditions. User sessions terminate after 8 hours of continuous connection. Idle sessions terminate after 30 minutes (remote access). Sessions terminate upon user logout or system restart.

4.9 Remote Access (3.1.12, 3.1.13, 3.1.14, 3.1.15)

Remote access to CUI systems is controlled, monitored, and encrypted.

4.9.1 Remote Access Authorization

Remote access requires explicit authorization from the IT Manager. Authorization documents business need for remote access. Remote access is granted for a defined period (maximum 1 year, renewable). Authorization is revoked upon role change or termination.

4.9.2 Remote Access Methods

Method	Status	Requirements
VPN (corporate)	Approved	MFA required, split tunneling disabled
Remote Desktop via VPN	Approved	VPN connection first, then RDP
Direct RDP to internet	Prohibited	Not allowed for CUI systems
SSH via VPN	Approved	VPN connection first, key-based auth preferred
Third-party remote tools	Prohibited	TeamViewer, AnyDesk, etc. not allowed for CUI

4.9.3 Remote Access Security

All remote access connections are encrypted using FIPS-validated cryptography. Remote access routes through managed access control points (VPN concentrator). Multi-factor authentication is required for all remote access. Remote sessions are logged with user, source IP, connection time, and duration.

4.9.4 Privileged Remote Access

Remote execution of privileged commands requires additional authorization documented in the access request. Remote privileged access is logged with commands executed. Remote access to security-relevant information (logs, configs) requires IT Manager approval.

> **SMB Implementation Tip:** A cloud-based VPN solution with MFA (e.g., a business firewall with built-in VPN) is often the most practical approach for SMBs. Ensure it supports logging.

4.10 Wireless Access (3.1.16, 3.1.17)

Wireless network access is authorized, authenticated, and encrypted.

4.10.1 Wireless Authorization

Wireless access to networks connected to CUI systems requires authorization. Wireless SSIDs and access points are documented in the network inventory. New access points require IT Manager approval before deployment. Personal/rogue access points are prohibited.

4.10.2 Wireless Security Requirements

Requirement	Specification
Encryption	WPA3-Enterprise or WPA2-Enterprise minimum
Authentication	802.1X with RADIUS, or WPA2-Enterprise with strong passphrase (20+ characters)
Guest network	Isolated VLAN, no access to CUI systems
SSID broadcast	May be hidden for corporate network
Access point hardening	Default credentials changed, firmware current

4.10.3 Wireless Monitoring

Wireless networks are monitored for rogue access points. Unauthorized access attempts are logged and investigated. Wireless access logs include device MAC, user (if 802.1X), and session duration.

4.11 Mobile Device Access (3.1.18, 3.1.19)

Mobile device connections to CUI systems are controlled and protected.

4.11.1 Mobile Device Authorization

Mobile devices accessing CUI require IT Manager authorization. Authorized devices are enrolled in Mobile Device Management (MDM). Personal devices (BYOD) require signed agreement acknowledging security requirements. Lost or stolen devices must be reported within 4 hours.

4.11.2 Mobile Device Security

Control	Requirement
Device encryption	Full-device encryption enabled
Screen lock	PIN (6+ digits) or biometric required
Auto-lock	2 minutes maximum
Remote wipe	Enabled via MDM
CUI storage	CUI encrypted at rest, in approved apps only
Jailbreak/root detection	Jailbroken devices blocked from access
App restrictions	Only approved apps may access CUI

4.12 External System Connections (3.1.20, 3.1.21)

Connections to external systems and use of external storage are controlled.

4.12.1 External System Access

Connections from CUI systems to external systems require risk assessment. External connections are documented with business justification. External connections use encrypted channels where technically feasible. User activity on external systems from CUI devices may be limited.

4.12.2 Portable Storage Devices

Scenario	Policy
USB drives on CUI workstations	Disabled by default; exceptions require IT Manager approval
Approved USB drives	Encrypted drives only; registered in asset inventory
USB drives on external systems	CUI not permitted on USB drives connected to external systems
External hard drives	Same policy as USB drives
Optical media (CD/DVD)	Disabled on CUI workstations

4.13 Publicly Accessible Content (3.1.22)

Controls prevent unauthorized posting of CUI to publicly accessible systems.

4.13.1 Public Posting Controls

CUI shall not be posted to publicly accessible systems without explicit authorization. Public-facing systems (websites, file shares) are reviewed quarterly for unauthorized CUI. Personnel are trained on what constitutes CUI and public posting risks. Automated scanning for CUI patterns on public systems is implemented where feasible.

4.13.2 Authorized Public Posting

If CUI must be made publicly accessible, authorization from Senior Management is required. Legal/contracts review confirms disclosure is permitted. CUI markings are applied appropriately. Access logging is enabled.

5. Access Reviews

Regular access reviews ensure access remains appropriate and identify accounts for removal.

5.1 Review Schedule

Review Type	Frequency	Reviewer	Scope
User access recertification	Quarterly	System/Data Owners	All active user accounts

Privileged account review	Monthly	IT Manager	All admin/privileged accounts
Service account review	Quarterly	IT Manager	All service accounts
Terminated user audit	Weekly	System Administrator	Confirm disabled within 24 hours
Remote access authorization	Semi-annually	IT Manager	All remote access users
Role definition review	Annually	IT Manager + Owners	All defined access roles

5.2 Review Process

System owners receive a list of users with access to their systems. Owners verify each user still requires access for their role. Access no longer required is marked for removal. System Administrator removes access within 5 business days. Review completion is documented with the date and the reviewer's signature.

6. Exceptions

Exceptions to this policy may be granted when technical or business constraints prevent compliance.

Exception requests must document the specific policy requirement that cannot be met, the business or technical reason for the exception, compensating controls that reduce the associated risk, the duration of the exception (maximum 1 year), and, if possible, the plan to achieve compliance.

Exceptions require approval from the IT Manager for non-privileged access controls and Senior Management for privileged access or controls protecting CUI. Approved exceptions are documented and tracked. Exceptions are reviewed at each access review cycle.

7. Enforcement

Violations of this policy may result in disciplinary action up to and including termination. Access violations are logged and investigated. Repeat violations result in escalating consequences. Intentional or malicious access violations may be referred for legal action. Violations that result in CUI compromise are reported per incident response procedures.

8. NIST 800-171 Control Mapping

This policy addresses the following NIST SP 800-171 Rev 2 Access Control requirements:

Control ID	Requirement	Policy Section
3.1.1	Limit system access to authorized users, processes, and devices	4.1
3.1.2	Limit access to authorized transactions and functions	4.1, 4.2

3.1.3	Control CUI flow per approved authorizations	4.3
3.1.4	Separate duties to reduce malevolent activity risk	4.4
3.1.5	Employ least privilege for security functions and privileged accounts	4.5
3.1.6	Use non-privileged accounts for non-security functions	4.5
3.1.7	Prevent non-privileged users from executing privileged functions	4.5
3.1.8	Limit unsuccessful logon attempts	4.6
3.1.9	Provide privacy and security notices	4.7
3.1.10	Use session lock with pattern-hiding displays	4.8
3.1.11	Terminate sessions after defined conditions	4.8
3.1.12	Monitor and control remote access sessions	4.9
3.1.13	Employ cryptographic mechanisms for remote access	4.9
3.1.14	Route remote access via managed access control points	4.9
3.1.15	Authorize remote privileged commands and security info access	4.9
3.1.16	Authorize wireless access prior to connection	4.10
3.1.17	Protect wireless access with authentication and encryption	4.10
3.1.18	Control connection of mobile devices	4.11
3.1.19	Encrypt CUI on mobile devices	4.11
3.1.20	Verify and control external system connections	4.12
3.1.21	Limit portable storage use on external systems	4.12
3.1.22	Control CUI on publicly accessible systems	4.13

9. Related Documents

Document ID	Document Name	Relationship
SSP-001	System Security Plan	Contains implementation details for all controls
POL-IA	Identification & Authentication Policy	Authentication requirements
POL-AU	Audit & Accountability Policy	Access logging and review
POL-SC	System & Communications Protection Policy	Encryption requirements
PRC-005	Access Management Process	Detailed account management steps
FRM-001	User Access Request Form	Access request template
FRM-002	Access Review Certification Form	Review documentation

10. Revision History

Version	Date	Author	Changes
1.0	March 1, 2026	Rachel Okafor	Initial policy

Document Approval

Role	Name	Signature	Date
IT Manager			
Senior Management			

Disclaimer: *This document is a customizable template. Organizations should review and adapt this policy for their specific environment, systems, and CUI handling requirements. This template does not constitute legal advice.*

Northgate Defense Systems, LLC	Document ID	[SSP-001]
	Version	
System Security Plan	Effective Date	March 1, 2026
	Document Owner	Rachel Okafor
	Approved By	David Whitfield

Table of Contents

1. Introduction

1.1 Purpose

This System Security Plan (SSP) describes the security controls implemented for Northgate CUI Enclave to protect Controlled Unclassified Information (CUI) in accordance with NIST SP 800-171 and CMMC Level 2 requirements. This document provides a comprehensive overview of the system's security posture and serves as the primary artifact for CMMC Level 2 assessment.

1.2 Scope

This SSP applies to all components within the defined CUI boundary that process, store, or transmit Controlled Unclassified Information in support of Department of Defense contracts. The scope includes:

• All hardware, software, and network components within the CUI boundary

• Personnel with access to CUI

• Physical locations where CUI is processed or stored

• External service providers that process CUI on behalf of the organization

1.3 System Overview

[Provide a brief description of the system, its purpose, and its role in supporting DoD contracts]

System Name:	Northgate CUI Enclave
System Type:	[General Support System / Major Application]
Operational Status:	[Operational / Under Development / Major Modification]
Primary Mission:	[Description]
CUI Categories:	[CTI / ITAR / Export Controlled / etc.]
CAGE Code:	[Code]
DUNS Number:	[Number]

2. System Environment

2.1 System Boundary

The CUI boundary encompasses all systems, networks, and physical locations where CUI is processed, stored, or transmitted. The boundary is defined to minimize the scope of compliance while ensuring all CUI handling is protected.

(Network diagram: CUI boundary encompassing the Northgate CUI Enclave)

2.1.1 Systems Within Boundary

System/Component	Function	CUI Handling
[Server Name]	CUI processing and storage	Process, Store, Transmit
[Workstations]	CUI processing and storage	Process, Store, Transmit
[Network Devices]	CUI processing and storage	[Transmit]
[Cloud Services]	CUI processing and storage	Process, Store, Transmit

2.1.2 Systems Outside Boundary

The following systems are explicitly outside the CUI boundary and do not process, store, or transmit CUI:

Corporate guest Wi-Fi; public marketing website

2.2 Network Architecture

[Describe network architecture including zones, segmentation, and data flows]

2.3 Data Flow

[Describe how CUI flows through the system - entry points, processing, storage, transmission, and exit points]

2.4 Physical Environment

Location	Type	CUI Activities	Physical Controls
1450 Crystal Drive, Arlington, VA 22202	[Office/Data Center]	[Description]	[Badge access, cameras, etc.]
1450 Crystal Drive, Arlington, VA 22202	[Remote/Home Office]	[Description]	[Controls in place]

3. Roles and Responsibilities

Role	Name	Responsibilities
Information System Owner	Rachel Okafor	Overall accountability for system security
Security Manager	Rachel Okafor	Day-to-day security operations and policy enforcement
System Administrator	Rachel Okafor	Technical implementation and maintenance of controls
Network Administrator	Rachel Okafor	Network security and monitoring
Security Assessor	Rachel Okafor	Internal assessment and compliance verification
Incident Response Lead	Rachel Okafor	Incident detection, response, and reporting

Privacy Officer	Rachel Okafor	CUI handling and privacy compliance

4. External Service Providers

The following external service providers process, store, or transmit CUI on behalf of the organization:

Provider	Service	FedRAMP Status	CUI Handling
[Microsoft]	[M365 GCC/GCC High]	[Authorized]	[Email, Files, Collaboration]
Microsoft Azure Government	Microsoft 365 GCC High	Implemented	[Description]
Microsoft Azure Government	Microsoft 365 GCC High	Implemented	[Description]

All external service providers have been verified to meet FedRAMP Moderate baseline or equivalent security requirements as required by DFARS 252.204-7012.

5. Security Control Implementation

This section documents the implementation status of all 110 NIST SP 800-171 security controls required for CMMC Level 2 certification. Each control includes the requirement text, implementation status, and description of how the control is implemented in this environment.

3.1 Access Control

This family contains 22 controls.

3.1.1 Authorized Access

Control Requirement:

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.2 Transaction & Function Control

Control Requirement:

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.3 CUI Flow Control

Control Requirement:

Control the flow of CUI in accordance with approved authorizations.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.4 Separation of Duties

Control Requirement:

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.5 Least Privilege

Control Requirement:

Employ the principle of least privilege, including for specific security functions and privileged accounts.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.6 Non-Privileged Access

Control Requirement:

Use non-privileged accounts or roles when accessing nonsecurity functions.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.7 Privileged Function Control

Control Requirement:

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.8 Unsuccessful Logon Attempts

Control Requirement:

Limit unsuccessful logon attempts.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.9 Privacy & Security Notices

Control Requirement:

Provide privacy and security notices consistent with applicable CUI rules.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.10 Session Lock

Control Requirement:

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.11 Session Termination

Control Requirement:

Terminate (automatically) a user session after a defined condition.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.12 Remote Access Control

Control Requirement:

Monitor and control remote access sessions.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.13 Remote Access Cryptography

Control Requirement:

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.14 Remote Access Routing

Control Requirement:

Route remote access via managed access control points.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.15 Privileged Remote Access

Control Requirement:

Authorize remote execution of privileged commands and remote access to security-relevant information.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.16 Wireless Access

Control Requirement:

Authorize wireless access prior to allowing such connections.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.17 Wireless Authentication

Control Requirement:

Protect wireless access using authentication and encryption.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.18 Mobile Device Control

Control Requirement:

Control connection of mobile devices.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.19 Mobile Device Encryption

Control Requirement:

Encrypt CUI on mobile devices and mobile computing platforms.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.20 External Connections

Control Requirement:

Verify and control/limit connections to and use of external systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.21 Portable Storage

Control Requirement:

Limit use of portable storage devices on external systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.1.22 Publicly Accessible Content

Control Requirement:

Control CUI posted or processed on publicly accessible systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.2 Awareness and Training

This family contains 3 controls.

3.2.1 Security Awareness

Control Requirement:

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.2.2 Security Training

Control Requirement:

Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.2.3 Insider Threat Awareness

Control Requirement:

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3 Audit and Accountability

This family contains 9 controls.

3.3.1 System Auditing

Control Requirement:

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.2 User Accountability

Control Requirement:

Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.3 Audit Review

Control Requirement:

Review and update logged events.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.4 Audit Failure Alerting

Control Requirement:

Alert in the event of an audit logging process failure.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID

environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.5 Audit Correlation

Control Requirement:

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.6 Audit Reduction

Control Requirement:

Provide audit record reduction and report generation to support on-demand analysis and reporting.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.7 Time Synchronization

Control Requirement:

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.8 Audit Protection

Control Requirement:

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.3.9 Audit Management

Control Requirement:

Limit management of audit logging functionality to a subset of privileged users.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4 Configuration Management

This family contains 9 controls.

3.4.1 Baseline Configurations

Control Requirement:

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.2 Security Configuration Settings

Control Requirement:

Establish and enforce security configuration settings for information technology products employed in organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.3 System Change Tracking

Control Requirement:

Track, review, approve or disapprove, and log changes to organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.4 Security Impact Analysis

Control Requirement:

Analyze the security impact of changes prior to implementation.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.5 Access Restrictions for Change

Control Requirement:

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.6 Least Functionality

Control Requirement:

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.7 Nonessential Functions

Control Requirement:

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.8 Application Execution Policy

Control Requirement:

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.4.9 User-Installed Software

Control Requirement:

Control and monitor user-installed software.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID

environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5 Identification and Authentication

This family contains 11 controls.

3.5.1 User Identification

Control Requirement:

Identify system users, processes acting on behalf of users, and devices.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.2 User Authentication

Control Requirement:

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.3 Multi-Factor Authentication

Control Requirement:

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.4 Replay-Resistant Authentication

Control Requirement:

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.5 Identifier Management

Control Requirement:

Prevent reuse of identifiers for a defined period.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.6 Identifier Disabling

Control Requirement:

Disable identifiers after a defined period of inactivity.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.7 Password Complexity

Control Requirement:

Enforce a minimum password complexity and change of characters when new passwords are created.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID

environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.8 Password Reuse

Control Requirement:

Prohibit password reuse for a specified number of generations.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.9 Temporary Passwords

Control Requirement:

Allow temporary password use for system logons with an immediate change to a permanent password.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.10 Cryptographic Key Protection

Control Requirement:

Store and transmit only cryptographically-protected passwords.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.5.11 Authenticator Feedback

Control Requirement:

Obscure feedback of authentication information.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.6 Incident Response

This family contains 3 controls.

3.6.1 Incident Handling

Control Requirement:

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.6.2 Incident Reporting

Control Requirement:

Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.6.3 Incident Response Testing

Control Requirement:

Test the organizational incident response capability.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID

environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.7 Maintenance

This family contains 6 controls.

3.7.1 System Maintenance

Control Requirement:

Perform maintenance on organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.7.2 Maintenance Control

Control Requirement:

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.7.3 Offsite Maintenance

Control Requirement:

Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.7.4 Media Inspection

Control Requirement:

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.7.5 Nonlocal Maintenance

Control Requirement:

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.7.6 Maintenance Personnel

Control Requirement:

Supervise the maintenance activities of maintenance personnel without required access authorization.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8 Media Protection

This family contains 9 controls.

3.8.1 Media Protection

Control Requirement:

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.2 Media Access

Control Requirement:

Limit access to CUI on system media to authorized users.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.3 Media Sanitization

Control Requirement:

Sanitize or destroy system media containing CUI before disposal or release for reuse.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.4 Media Marking

Control Requirement:

Mark media with necessary CUI markings and distribution limitations.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.5 Media Transport Access

Control Requirement:

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.6 Media Transport Cryptography

Control Requirement:

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.7 Removable Media Control

Control Requirement:

Control the use of removable media on system components.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.8 Shared Media

Control Requirement:

Prohibit the use of portable storage devices when such devices have no identifiable owner.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.8.9 Media Backup

Control Requirement:

Protect the confidentiality of backup CUI at storage locations.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.9 Personnel Security

This family contains 2 controls.

3.9.1 Personnel Screening

Control Requirement:

Screen individuals prior to authorizing access to organizational systems containing CUI.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.9.2 Personnel Termination

Control Requirement:

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.10 Physical Protection

This family contains 6 controls.

3.10.1 Physical Access

Control Requirement:

Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.10.2 Facility Protection

Control Requirement:

Protect and monitor the physical facility and support infrastructure for organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.10.3 Visitor Escort

Control Requirement:

Escort visitors and monitor visitor activity.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.10.4 Physical Access Logs

Control Requirement:

Maintain audit logs of physical access.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.10.5 Physical Access Devices

Control Requirement:

Control and manage physical access devices.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.10.6 Alternate Work Sites

Control Requirement:

Enforce safeguarding measures for CUI at alternate work sites.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.11 Risk Assessment

This family contains 3 controls.

3.11.1 Risk Assessment

Control Requirement:

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.11.2 Vulnerability Scanning

Control Requirement:

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.11.3 Vulnerability Remediation

Control Requirement:

Remediate vulnerabilities in accordance with risk assessments.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.12 Security Assessment

This family contains 4 controls.

3.12.1 Security Control Assessment

Control Requirement:

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.12.2 Plans of Action

Control Requirement:

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.12.3 Continuous Monitoring

Control Requirement:

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.12.4 System Security Plan

Control Requirement:

Develop, document, and periodically update system security plans that describe system boundaries, system environments of

operation, how security requirements are implemented, and the relationships with or connections to other systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13 System and Communications Protection

This family contains 16 controls.

3.13.1 Boundary Protection

Control Requirement:

Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.2 Security Architecture

Control Requirement:

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.3 Role Separation

Control Requirement:

Separate user functionality from system management functionality.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.4 Shared Resource Control

Control Requirement:

Prevent unauthorized and unintended information transfer via shared system resources.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.5 Public Access Protections

Control Requirement:

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.6 Network Exceptions

Control Requirement:

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.7 Split Tunneling

Control Requirement:

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.8 Cryptographic Protection

Control Requirement:

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.9 Network Disconnect

Control Requirement:

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.10 Cryptographic Keys

Control Requirement:

Establish and manage cryptographic keys for cryptography employed in organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.11 FIPS Cryptography

Control Requirement:

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.12 Collaborative Device Control

Control Requirement:

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.13 Mobile Code

Control Requirement:

Control and monitor the use of mobile code.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.14 VoIP

Control Requirement:

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.15 Session Authenticity

Control Requirement:

Protect the authenticity of communications sessions.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.13.16 Data at Rest

Control Requirement:

Protect the confidentiality of CUI at rest.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.14 System and Information Integrity

This family contains 7 controls.

3.14.1 Flaw Remediation

Control Requirement:

Identify, report, and correct system flaws in a timely manner.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.14.2 Malicious Code Protection

Control Requirement:

Provide protection from malicious code at designated locations within organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.14.3 Security Alerts

Control Requirement:

Monitor system security alerts and advisories and take action in response.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.14.4 Malicious Code Updates

Control Requirement:

Update malicious code protection mechanisms when new releases are available.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.14.5 System Scanning

Control Requirement:

Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.14.6 Inbound Traffic Monitoring

Control Requirement:

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

3.14.7 Unauthorized Use Detection

Control Requirement:

Identify unauthorized use of organizational systems.

Implementation Status:

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Not Applicable

Implementation Description:

Northgate Defense Systems, LLC satisfies this requirement through the corresponding control-family policy and standardized operating procedures included in this suite. Implementation is enforced across the Microsoft 365 E5 and Microsoft Entra ID environment, with supporting evidence retained in the central compliance repository.

Responsible Party:

Information Security Manager

6. Plan of Action and Milestones

Controls that are not fully implemented are tracked in the Plan of Action and Milestones (POA&M). The current POA&M status is:

Control ID	Status	Milestone	Target Date	Responsible
[ID]	Implemented	[Description]	March 1, 2026	Rachel Okafor
[ID]	Implemented	[Description]	March 1, 2026	Rachel Okafor
[ID]	Implemented	[Description]	March 1, 2026	Rachel Okafor

The complete POA&M is maintained separately and updated monthly. Reference: [POA&M Document ID]

7. System Interconnections

The following systems have authorized connections to this system:

Connected System	Organization	Connection Type	Data Exchanged	Agreement
Northgate CUI Enclave	Northgate Defense Systems, LLC	VPN	Controlled Technical Information (CTI)	ISA
Northgate CUI Enclave	Northgate Defense Systems, LLC	VPN	Controlled Technical Information (CTI)	ISA

8. Incident Response

8.1 Incident Response Capability

The organization maintains an incident response capability in accordance with NIST SP 800-61 and DFARS 252.204-7012 requirements. The incident response plan is documented in [IR Plan Document ID].

8.2 Incident Reporting

Cyber incidents affecting CUI or covered contractor information systems are reported to the DoD within 72 hours of discovery via the DC3 portal (https://dibnet.dod.mil).

8.3 Incident Response Contacts

Role	Name	Phone	Email
Primary IR Contact	Rachel Okafor	+1 (703) 555-0142	security@northgate-defense.example
Alternate IR Contact	Rachel Okafor	+1 (703) 555-0142	security@northgate-defense.example
Management Escalation	Rachel Okafor	+1 (703) 555-0142	security@northgate-defense.example

9. SSP Approval

This System Security Plan has been reviewed and approved by the following authorities:

Information System Owner:	
Signature:	
Date:	

Authorizing Official:	
Signature:	
Date:	

Disclaimer: *This System Security Plan template is provided for guidance purposes. Organizations should customize this document to accurately reflect their specific system environment, security controls, and compliance requirements.*