NEOMED OPERATIONAL POLICY	Policy No: 3349-OP-361
OPERATIONAL POLICY TITLE: Information Security Program	EFFECTIVE DATE: July 10, 2019 REVISED DATE: June 9, 2023
RESPONSIBLE DEPARTMENTS: Information Technology	Approval Authority: Vice President, Operations & Finance

(A) PURPOSE

Northeast Ohio Medical University ("NEOMED") has instituted the following Information Security Program Policy to document the enterprise Information Security Program ("Program") used to reasonably manage and safeguard University Data and Systems as well as maintain compliance with the Information Security requirements of applicable laws and regulations.

(B) SCOPE

This Policy applies to University Data and Systems as well as any individual or Service Provider that may access, use, transmit, dispose of, or receive University Data and/or Systems.

(C) DEFINITIONS

(1) "Authorization" refers to the granting of permission to an identified individual to use University Data or System(s) and to explicitly accept the Risk to University operations, individuals, and assets based on extending such permission. Acceptance of Authorization to use University Data and Systems establishes an obligation on the part of the individual to use those resources responsibly.

(2) "Availability" refers to the ensuring of timely and reliable access to and use of Data or Systems. A loss of availability is the disruption of access to or use of Data or Systems (e.g., hard drive failure, destruction of a System, System unresponsiveness, denial of service attack).

(3) "Confidentiality" refers to the preservation of authorized restrictions on Data access and disclosure, including means for protecting personal privacy and proprietary Data and Systems. A loss of Confidentiality is the unauthorized disclosure of Data (e.g., compromised by hackers; released or published publicly without Authorization).

(4) "Consumer" refers to an individual who obtains or has obtained a financial product or service from the University that is to be used primarily for personal, family, or household purposes, or that person's legal representatives.

(5) "Customer" refers to a Consumer who has established a continuing relationship with the University.

(6) "Customer Information" refers to any record containing Personally Identifiable Financial Information (or any record derived from Personally Identifiable Financial Information that is not publicly available) about a Customer of NEOMED, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of NEOMED or its affiliated entities. (e.g., name; addresses; payment history; tuition and/or financial aid records; bank account numbers; income; loan balances; and Social Security numbers). Customer Information is considered University Data.

(7) "Data" refers to any instance of information, regardless of form or storage medium, that is categorized by an organization or by a specific law or regulation.

(8) "Data Steward" is defined within Section (D)(2)(e)(i) of this Policy.

(9) "Information Security" refers to the protection of University Data and Systems from unauthorized access, use, disclosure, disruption, modification and destruction with the intent to provide Confidentiality, Integrity and Availability to such Data and Systems.

(10) "Qualified Individual" is defined within Section (D)(2)(b) of this Policy.

(11) "Integrity" refers to the guarding against improper Data or System modification or destruction and ensuring authenticity and non-repudiation in the use of Data or Systems. A loss of Integrity is the unauthorized modification or destruction of Data or Systems where such resources can no longer be trusted for use, are not complete, or incorrect.

(12) "Personally Identifiable Financial Information" refers to any information a student or other third party provides to obtain a financial product or service from NEOMED, any information about a student or other third party resulting from any transaction with NEOMED involving a financial service, or otherwise obtained about a student or other third party in connection with providing a financial service to that person.

(13) "Private University Data" refers to University Data used to conduct University business for which access must be guarded due to legal, regulatory, administrative, and contractual requirements, in addition to proprietary, ethical, or privacy considerations.

(14) "Record" refers to any document, device, or item, regardless of physical form or characteristic, including an Electronic Record, that is created, received by, or comes under the jurisdiction of the University which serves to document the organization, its functions, policies, decisions, procedures, operations or other activities of the University.

(15) "Risk", with respect to the University, refers to the effect of uncertainty, positive or negative, on the University's strategy and its strategic objectives.

(16) "Restricted University Data" refers to University Data that requires the highest level of protection due to legal, regulatory, administrative, contractual, rule, industry standards, or policy requirements.

(17) "Security Incident" refers to an adverse event that results in a suspected or known unauthorized disclosure, misuse, alteration, destruction, or other compromise of University Data or Systems. A Security Incident is caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms through nonelectronic means (e.g., a violation of applicable University Policies, mishandled documents, the theft or loss of a System, verbal or visual disclosure of personal information) and electronic means (e.g., hacking, malware, ransomware, phishing).

(18) "Service Provider" refers to any person or entity that receives, maintains, processes, or otherwise is permitted access to University Data and/or Systems through its provision of services directly to NEOMED.

(19) "System" refers to an information technology resource that can be classified, may have security controls applied, and is organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of University Data. Example of Systems are, but not limited to desktop, laptop, or server computers; mobile devices (e.g., iPhones; iPads; Android; BlackBerry) to the extent that they interact with University Data and Systems, such as University email; University network(s); software; applications; and databases.

(20) "System Steward" is defined within Section (D)(2)(f)(i) of this Policy.

(21) "Threat" refers to the potential for a particular circumstance or event to cause harm to University Data and Systems by successfully exercising a particular flaw or weakness that can be accidentally triggered or intentionally exploited, which may result in a Security Incident.

(22) "University Data" refers to Data that is created, collected, stored and/or managed in association with fulfilling the University's mission or its required business functions. University Data may or may not constitute a Public Record (as defined within Ohio Revised Code §149.43).

(23) "User" refers to any individual or Service Provider that has received Authorization, if applicable, to access, use, transmit, dispose of, or receive University Data and/or Systems.

(D) POLICY STATEMENT

(1) Overview

(a) Northeast Ohio Medical University's Information Security Program ("ISP") is a combination of policy, security architecture design, and descriptions of current Information Security services and control procedures. When integrated, the ISP describes administrative, physical, and technical security safeguards to effectively manage Information Security Risks to the University's assets and community. These Risks include those related to the access, collection, distribution, processing, protection, storage, use, transmission, disposal, or otherwise handling of University Data and Systems.

(b) NEOMED's ISP provides institutional value by enabling the delivery of Information Technology to more individuals, in a timelier manner, with University Data and Systems necessary to achieve the University's mission. Appropriate Information Security is crucial to the University so that Risks inherent to a distributed, open technology environment can be managed accordingly.

(c) NEOMED's ISP was designed to be appropriate based upon the University's size, complexity, and the nature of its activities.

(d) The ISP is achieved by the facilitating the following components:

(i) Outlining the University's governance, methods and principles for administering and managing Information Security, including designating an employee or employees responsible for coordinating the ISP;

(ii) Determining the appropriate classification and corresponding security controls for University Data and Systems;

(iii) Supplementing the University's evolving Risk management process by assessing, responding to, and managing reasonably foreseeable Risks to the security, Confidentiality, Availability and Integrity of University Data and Systems. These Risk assessments enable the University community to be more aware of such Risks, identify controls to mitigate those Risks,

and understand the residual Risks that remain after identified controls and safeguards have been implemented;

(iv) Designing and implementing safeguards to control the Risks identified and that the effectiveness of these safeguards is regularly tested and monitored, including any revised or new policies, procedures and training;

(v) Ensuring continuity of University services and mitigate University Data and System loss or compromise;

(vi) Enhancing Information Security Incident response management to enable the University to recover its information technology assets in lieu of disaster or Security Incident more quickly and to more effectively reduce the damage to the University community.

(vii) Overseeing Service Providers and satisfy the University's legal and contractual responsibilities regarding Information Security.

(viii) Maintaining and adjusting the Information Security Program based upon the results of testing and monitoring conducted, the sensitivity of and Risks related to University Data and Systems, and internal or external Threats to Information Security.

(e) With these components, the University's ISP intends to:

(i) Ensure the security, Confidentiality, Availability and Integrity of University Data and Systems, if applicable;

(ii) Protect against anticipated Threats or hazards to the security or Integrity of University Data and Systems; and

(iii) Protect against unauthorized access to or use of University Data and Systems, which could result in substantial harm or inconvenience to the University community.

(f) The University's Information Security efforts, to which the ISP contributes, seeks to align to the Center for Internet Security Critical Security Controls ("CIS Controls"), which has been widely adopted by institutions across the United States. The CIS Controls provide a

framework for cybersecurity management, including asset identification, System protection, Threat detection, and Security Incident response and recovery. These efforts will evolve over time as the University's Information Security Program matures. Additionally, the University will leverage other frameworks (e.g., NIST 800-171) where appropriate based on the types of University Data and Systems subject to certain federal and state regulations.

(g) Unless specified otherwise by University policy, individual divisions, departments and offices can develop more stringent local policies and procedures that address specific local issues. These areas may develop policies and procedures tailored to their environment that address areas not covered by University policy. If a division, department or office chooses to keep or develop local Information Security policies or procedures, those policies and procedures are valid only to the extent that they are more stringent than the requirements contained in the University Information Technology policies, which constitute the mandatory baseline.

(h) Given the nature of the ISP, relevance to the continuation of the University's mission, and the severity of Risk that could result from an unauthorized disclosure of University Data, Records containing University Data regarding ISP Risks and safeguards shall be handled as Private University Data.

(i) The enforcement of the ISP will be administered in accordance with the *Information Security Policy* and/or *Acceptable Use of University Data and Systems Policies*, as applicable.

(2) Information Security Roles

(a) Overview

(i) The ISP's organizational structure was designed considering the University's distributed environment; as such, all Users have a responsibility to ensure appropriate Information Security controls and procedures are practiced within their areas of responsibility.

(ii) The roles and responsibilities within the ISP are described below. Additional roles and responsibilities may be added or combined based on local departmental or office needs.

(b) Qualified Individual

(i) Federal regulations and associated statutes require the University to designate a Qualified Individual responsible for overseeing, implementing and enforcing the institution's ISP. The Director of Information Security has been identified as the Qualified Individual of the University.

(ii) The Qualified Individual will:

(a) Serve as point-of-contact for the University's Information Security efforts;

(b) Understand the ISP, corresponding laws, regulations, and other applicable policies;

(c) Coordinate the assessment, management, and mitigation of Information Security Risks;

(d) Develop, disseminate, and enforce policies and procedures related to Information Security;

(e) Respond to Security Incidents as they occur;

(f) Assist in outreach, training and educational awareness regarding Information Security matters;

(g) Review technology agreements to determine the implications of contractual terms that are related to University Data, in consultation with the Office of General Counsel;

(h) Administer and manage the University's cyber liability insurance program; and

(i) Provide guidance to the University, divisions, departments and offices to meet or maintain compliance with applicable policies, procedures, laws, and regulations.

(c) Information Technology personnel

(i) Personnel within the University's Information Technology ("IT") department are responsible for providing a secure technology infrastructure in support of University Data and Systems, including, but not limited to, providing digital security, backup and recovery processes, granting access privileges as authorized by Data and System Stewards (if applicable), and implementing and administering applicable security controls over University Data and Systems.

(ii) Additional responsibilities of IT personnel include:

(a) Monitoring the use of University Data and Systems, including communications that use the University network(s) for transmission or storage;

(b) Documenting and implementing audit mechanisms, timing of log reviews and log retention periods;

(c) Disconnecting, disabling, or separating University Data and Systems from the University network or Users in lieu of a Threat or other Information Security Risk;

(d) Erasing or preventing access to all University Data Stored on University Systems previously used for University business, as requested or required;

(e) Working with System Stewards and Data Stewards to aggregate an inventory of all Systems and Data, respectively;

(f) Conducting periodic vulnerability scanning of any University Systems connected to the University network(s); and

(g) Monitoring and reporting metrics to the Qualified Individual for any potential Risk mitigation actions.

(d) Data Stewards

(i) Data Stewards are University personnel who are responsible for the management and oversight of Data within their area(s) of responsibility,

to provide authorized Users with University Data that is easily accessible in a consistent manner.

(ii) Data Stewards are identified by the director, department head or manager of a given department or office in conjunction with the Qualified Individual. Those identified could serve as other roles outlined within this Policy, if appropriate and applicable.

(iii) Additional responsibilities of Data Stewards include:

(a) Ensuring the appropriate minimum University Data security controls are implemented for which they have oversight;

(b) Evaluating and classifying University Data in their respective areas, consistent with the University's *Classification of University Data and Systems Policy*;

(c) Helping communicate University Data-related policies and procedures across the University;

(d) Providing Authorization to University Data for which they have oversight, which may involve working with Information Technology personnel;

(e) Contributing to the Information Security Risk management process, which includes assessing and monitoring Risks within their area and reporting such Risks and controls to the Qualified Individual.

(f) Collaborating with the Qualified Individual and IT personnel in developing a University Data inventory; and

(g) Reporting suspected misuse or other related Information Security Incidents, consistent with the *Information Security Incident Response Plan Policy*.

(e) System Stewards

(i) System Stewards are University personnel who are responsible for the management and oversight of University System(s) within their area(s) to provide Authorization and support to Users.

(ii) System Stewards are identified by the director, department head or manager of a given department or office in conjunction with Qualified Individual. Those identified could serve as other roles outlined within this Policy, if appropriate and applicable.

(iii) Additional responsibilities of System Stewards include:

(a) Ensuring appropriate minimum University System security controls are implemented for which they have oversight;

(b) Evaluating and classifying University Systems in their respective areas, consistent with the University's *Classification of University Data and Systems Policy*;

(c) Helping communicate University System-related policies and procedures across the institution;

(d) Providing Authorization to University Systems for which they have oversight, which may involve working with Information Technology personnel;

(e) Contributing to the Information Security Risk management process, which includes assessing and monitoring Risks within their area and reporting such Risks and controls to the Qualified Individual;

(f) Collaborating with the Qualified Individual and IT personnel in developing a University Data inventory; and

(g) Reporting suspected misuse or other related Information Security Incidents, consistent with the *Information Security Incident Response Plan Policy*.

(f) Users

(i) Users are responsible for ensuring that University Data and Systems are used in compliance with the *Acceptable Use of University Data and Systems Policy* and other Information Technology policies, laws and regulations.

(3) Risk Identification and Assessment

(a) The ISP incorporates the identification and assessment of reasonably foreseeable external and internal Risks to the security, Confidentiality, Availability and Integrity of University Data and Systems that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromises of such Data and Systems.

(b) NEOMED recognizes that it faces both internal and external Risks. These Risks include, but is not limited to:

(i) Unauthorized access of University Data by someone other than the owner of such Data;

(ii) Compromised University System security because of system access by an unauthorized person or third party;

(iii) Loss of University Data Confidentiality, Integrity or Availability;

(iv) Physical loss of University Data in a disaster;

(v) Errors introduced into University Systems;

(vi) Corruption of University Data and/or Systems;

(vii) Interception of University Data during transmission; and

(viii) Unauthorized access of, unauthorized requests for and unauthorized transfer through third parties of University Data.

(c) The Qualified Individual will provide guidance to appropriate personnel in University departments and offices in evaluating their current procedures and in assessing reasonably foreseeable Risks to University Data and Systems in their respective areas.

(d) Risks identified will be documented within the NEOMED IT Risk Register, wherein such Risks will be prioritized and risk mitigations/safeguards will be documented. At a minimum, safeguards addressing the following security controls will be included:

(i) Reviewing access controls and limiting access only to authorized users and the information they need to perform their duties and functions;

(ii) Identifying and maintaining a current inventory of the Data, personnel, devices, Systems, and facilities involved;

(iii) Where required, encrypting University Data (e.g., Customer Information) in transit over external networks and at rest;

(iv) Adopting secure development practices for any applications in use, where applicable;

(v) Implementing Multi-factor Authentication for any User accessing University Systems;

(vi) Implementing data retention and disposal procedures and policies;

(vii) Implementing change management procedures and controls; and

(viii) Implementing procedures and controls to monitor and log the activity of authorized Users and detect unauthorized access.

(4) Safeguards and Monitoring

(a) Through the ISP, the Qualified Individual will coordinate with appropriate personnel, to monitor and reevaluate existing safeguards as well as allow for the development and implementation of safeguards to control Risks identified in assessments.

(5) Employee Training and Management

(a) Safeguards for this ISP include the management and training of those individuals with authorized access to University Data and Systems.

(b) The Qualified Individual will collaborate with appropriate personnel to identify categories of positions, Employees or others who have access to University Data and Systems.

(c) Employees that regularly work with University Data and Systems are required to be trained on Information Security to help minimize Risk and safeguard such Data. Information Security training includes controls and guidance on how to avoid

unauthorized disclosures and access to University Data and Systems.

(i) Additional training may be required for handling Restricted University Data pursuant to specific legal, regulatory, administrative, or contractual requirements. Users should consult their supervisor, departmental manager or the Qualified Individual regarding additional and ongoing training needs.

(d) These training efforts are supplemental by regular Information Security awareness articles posted on and communicated through the University's internal communication platform. Such communications include including changes to existing Information Security policies and procedures as well as new policies, procedures, or efforts related to the safeguarding of University Data and Systems.

(e) Additionally, guidance is provided to Employees regarding the proper management of University Records and how to properly dispose of Records that contain University Data in accordance with the University's Records Retention Schedule.

(6) Access Control and Authorization

(a) Authorization to use University Data and Systems are privileges are granted by Data Stewards and System Stewards, respectively, who are entrusted with responsibility and management of such University Data and Systems. Such authorization is limited to authorized persons for business purposes only.

(i) Business purposes are those consistent with both the broad educational, research, and service goals of the University and the person's or Service Provider's relationship with the University (e.g., employment, contractual responsibilities).

(ii) All Users that require access to Private/Restricted University Data or High-Risk Systems must receive approval by Data Stewards and System Stewards to access such Data and Systems, respectively.

(b) Acceptance of Authorization to use University Data and Systems establishes an obligation on the part of the User to use these resources responsibly and in conformity with all federal and state laws, regulations and applicable University policies and procedures.

(7) Physical Security

(a) NEOMED addresses the physical security of University Data and Systems by limiting access only to those Employees who have a legitimate business reason to handle such Data and Systems.

(b) Additionally, each department or office responsible for maintaining University Data is instructed to take steps to protect that Information from loss, destruction or damage due to environmental hazards, such as fire and water damage or technical failures.

(c) University buildings that house University Systems must be protected with security measures that prevent unauthorized persons from gaining access in accordance with the University's *Access and Use of University Owned Buildings* and *Security and Access Policies*.

(d) When delivering Private or Restricted University Data on physical devices or paper, such Data should only be delivered to secure locations (e.g., an access-controlled facility or building). When not in use, such Data must be stored in locked enclosures.

(8) University Systems

(a) University Systems are critical to the processing, storage, transmission, retrieval and disposal of University Data, including protected information within federal and state regulations, such as Customer Information.

(b) University Systems will be reasonably designed to limit the Risk of unauthorized access to University Data. This includes limiting Authorization to access University Systems, maintaining appropriate screening programs to detect technological intrusions, malware and viruses, and implementing security patches and fixes to address identified vulnerabilities.

(c) Social Security numbers are considered protected information under both the Gramm-Leach-Bliley Act ("GLBA") and the Family Educational Rights and Privacy Act ("FERPA"). As such, NEOMED does not utilize Social Security numbers as student identifiers and instead utilizes student identification numbers within the University's enterprise resource planning System. By necessity, student Social Security numbers will remain in the University's enterprise resource planning System; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

(9) Managing System Failures and Attacks

(a) The University will maintain effective Systems and related mechanisms to prevent, detect, and respond to attacks, intrusions and other System failures. Such failures will be addressed by the IT department and, if needed, with external support.

(b) In accordance with state and federal laws and regulations, the University must have an incident response plan in place to record, report and respond to Security Incidents. As such, the University has developed an *Information Security Incident Response Plan Policy*, which provides guidance for the identification, containment, notification, verification, investigation and remediation of such Security Incidents.

(c) All Users are obligated to report any known or perceived Security Incidents, including violations to the ISP, unauthorized disclosures of University Data or any supporting University policies, as described within the *Information Security Incident Response Plan Policy*.

(10) Monitoring and Testing

(a) Monitoring of existing Information Security safeguards may be accomplished through existing University processes and Systems, including network monitoring, IT ticket escalation procedures and other University Risk management efforts.

(b) Based upon the Risks identified and the residual Risks that result from implementing safeguards, the University will develop, revise and adopt policies and procedures on an ongoing basis to appropriately safeguard the security, Confidentiality, Availability and Integrity of University Data, including Customer Information.

(11) Service Providers

(a) Federal and state laws and regulations require the University to take reasonable steps to select and retain Service Providers who maintain appropriate safeguards for certain University Data, such as Customer Information. As such, the University must require, by contract or agreement, that security controls and safeguards will be used to protect University Data and Systems, consistent with the classification of University Data being processed, Risk classification of the University System

and the services being provided by the Service Provider.

(b) These security controls and safeguards shall implement protections aligned with University policies and industry standards and include physical, electronic, and procedural safeguards to protect University Data and Systems supplied to the Service Provider, including prompt Security Incident reporting procedures.

(c) As a part the ISP, the Qualified Individual, in conjunction with the Office of the General Counsel and the Office of Accounting & Budget, will institute methods for selecting and retaining Service Providers that can maintain appropriate safeguards for University Data, including Customer Information.

(d) Additionally, the Qualified Individual will work with the Office of the General Counsel to develop and incorporate standard, contractual provisions for Service Providers that will require such Providers to implement and maintain appropriate safeguards.

(e) The University may request the Service Provider to specify, in writing, their security controls and the ways in which University Data and Systems will be safeguarded.

(12) ISP Communication, Evaluation and Adjustment

(a) The Qualified Individual will evaluate and adjust the ISP as needed, based on results of any security control testing, the Risk identification and assessment activities undertaken pursuant to the ISP, as well as any material changes to the University's operations or other circumstances that may have a material impact on the ISP.

(b) The Qualified Individual will provide an annual written report to the Board of Trustees regarding the overall status and progress of the University's ISP.

(13) Legal and Regulatory Compliance Requirements

(a) The University continuously aims to comply with the Information Security requirements of all applicable laws and regulations, including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA"); the Gramm-Leach-Bliley Act ("GLBA"); and the Payment Card Industry Data Security Standards ("PCI-DSS").

(b) The Gramm-Leach-Bliley Act is a law, enforced by the Federal Trade Commission,

that applies to financial institutions seeking to protect Consumer financial privacy (the "Privacy Rule") and safeguard how Customer Information is collected, stored and used (the "Safeguards Rule"). Higher education institutions, including NEOMED, are considered financial institutions under the GLBA due to their role in servicing student loans.

(i) Higher education institutions are deemed to be in compliance with the GLBA's Privacy Rule if they are in compliance with FERPA.

(ii) The ISP as outlined within this Policy is in accordance with the requirements of the GLBA's Safeguards Rule.

(c) Please refer to the University's Policy Portal and FERPA website (https://www.neomed.edu/registrar/ferpa/) for more information on the University's compliance with these requirements.