



Norwich University Information Assurance Security Policy

Final Version 9.2 for Implementation

Table of Contents

| | |
|---|---|
| 1.0 Introduction..... | 2 |
| 2.0 Information Security Responsibilities..... | 2 |
| 2.1 Chief Information Security Officer | 3 |
| 2.2 Information Technology (IT)..... | 3 |
| 2.3 Worker Status Changes..... | 3 |
| 2.4 Internal Audit Function..... | 4 |
| 3.0 Statements of Policy | 4 |
| 3.1 Use of Information | 4 |
| 3.2 Policy Conflicts..... | 4 |
| 3.3 Authority to Create Standards and Practices under this Policy | 4 |
| 3.4 Expectation of Privacy..... | 5 |
| 3.5 Data and Program Damage Disclaimers..... | 5 |
| 3.6 Industry-Specific Information Security Standards | 5 |
| 3.7 Security Testing..... | 6 |
| 3.8 Incident Response..... | 6 |
| 3.9 Policy Non-Enforcement | 6 |
| 3.10 Consequences of Non-Compliance | 6 |
| 3.11 Legal Conflicts | 7 |
| 3.12 Contacting Law Enforcement | 7 |
| 3.13 Disclosure of Information to Law Enforcement | 7 |
| 3.14 Temporary Accounts | 7 |
| 3.15 Viruses and Other Security Incidents | 7 |
| 3.16 Software Development Source..... | 8 |
| 3.17 Email Acceptable Use..... | 8 |
| 3.18 Information Security Classification..... | 8 |
| 3.19 Loss or Disclosure of Sensitive Information..... | 9 |
| 3.20 Change Control..... | 9 |
| 3.21 Security Products and Services | 9 |
| 3.22 Centralized Information Security | 9 |

1.0 Introduction

Developing, implementing, communicating and updating Information Assurance (IA) security policies is vital to assuring that Norwich University is in compliance with legal requirements and to manage employees, students, third party businesses and vendors effectively.

Additionally, this policy helps to ensure that Norwich University is able to support further growth of the organization, and that its business practices provide a consistently high level of customer, supplier, employee, student and business-partner service. This document is also intended to support the organization's reputation for high-integrity and high-quality educational and business dealings. Because prevention of security problems is considerably less expensive than correction and recovery, this policy will help reduce costs in the long run.

A single unauthorized exception to security measures can jeopardize other users, the entire organization, and even outside organizations such as academic and business partners. The interconnected nature of information systems requires that all employees and students observe a minimum level of security. This document defines that minimum level of due care. As a condition of continued employment or enrollment, all employees, students, contractors, consultants, and temporaries must consistently observe the requirements set forth in this document.

2.0 Information Security Responsibilities

The responsibility of Information Technology managers (the VPAA, CISO, and key IT staff) is to conduct business within their departments in such a way as to add value to the organization. Management provides the essential framework for accomplishing technical work as well as assuring the security of data and information. Information Technology (IT) managers ensure the consistent functioning of the organizational computing environment. Ideally, they also provide insights and guidance to upper management in strategic planning to take advantage of new opportunities.

All managers must ensure that information security within their departments is treated as a regular business problem to be faced and solved and they are responsible for promoting security as everyone's business.

Managers have a number of information security related responsibilities:

- Avoiding the loss of information and data.
- Enabling business functions.
- Ensuring that information security policies and technology support, rather than hinder, the principal business and function of the organization.

- Helping to achieve strategic goals of the organization.
- Making decisions about business processes.

2.1 Chief Information Security Officer

The Chief Information Security Officer (CISO) is the University's designated authority for all information security related matters. The CISO is the direct representative of the Vice President for Academic Affairs (VPAA) in all information security related matters and acts under the authority of the VPAA, this policy, and related standards and practices.

2.2 Information Technology (IT)

The Information Technology department is the central point of contact for all information security matters at Norwich University. Acting as internal technical consultants, it is this department's responsibility to create workable information security practices that takes into consideration the needs of users and selected third parties. Reflecting these practices, this department defines information security standards, procedures, and other requirements applicable to the entire organization. IT must handle all access control administration activities, monitor the security of Norwich University information systems, and provide information security training and awareness programs to Norwich University employees.

The department is responsible for periodically providing management with reports about the current state of information security at Norwich University. The IT department must provide technical consulting assistance related to emergency response procedures and disaster recovery. The IT department is also responsible for organizing a computer incident response team (CIRT) to respond promptly to virus infections, hacker attacks and breaches of the network, system outages, violations of law involving the use of University computing resources (e.g., presence of child pornography) and similar information security problems.

In all cases where information security is involved, the Chief Information Security Officer must be notified immediately and no action except emergency response may be taken without his/her specific approval

2.3 Worker Status Changes

Every change in the employment status of Norwich University employees, consultants, contractors, and temporary employees, must be reported immediately by applicable management to Human Resources, who must subsequently notify the Information System Administrator involved. Upon a change in status the employee or temporary worker information systems access credentials will be reviewed and changed as necessary. If an employee or temporary worker is terminated, his/her information system access credentials will be deactivated. It is not necessary to remove those accounts immediately unless there is a specific reason to do so (e.g., involuntary termination for wrongdoing). However, accounts remaining unused for a period of one year after deactivation may be deleted.

An employee's immediate manager must approve a request for system access based on existing job profiles. If a job profile does not exist, it is the manager's responsibility to create the profile, obtain the approval and inform the IT department. User IDs are specific to individuals, and must not be reassigned to, or used by, others. Shortly after the employee's separation from Norwich University, the manager is additionally responsible for reassigning the involved files to other staff.

2.4 Internal Audit Function

The responsibility of an Internal Audit function is to perform compliance checks periodically to ensure that all parties are performing their assigned duties, and to ensure that other information security requirements are being consistently observed. Internal Audit informs top management, ensuring that internal controls, including those related to information security, are consistent with both top management expectations and University goals.

3.0 Statements of Policy

3.1 Use of Information

Information is a critical and vital asset, and all accesses to, uses of, and processing of Norwich University information must be consistent with Norwich University policies and standards.

Norwich University information must be used only for the business processes and educational and organizational purposes expressly authorized by management or authorized persons.

3.2 Policy Conflicts

Where this policy conflicts with another existing and accepted Norwich University policy concerning an issue that is not specific to information assurance and security, the preexisting policy will prevail. If the conflict is directly related to information assurance and security, this policy will prevail. If a preexisting policy has not been fully accepted or is in draft form, this policy will prevail.

3.3 Authority to Create Standards and Practices under this Policy

This policy explicitly grants authorization to create standards, practices and procedures in support of the policy under the guidance and approval of school or department managers, Deans and other senior university administrators. When so created, reviewed and accepted through due process, these standards, practices and procedures have the same authority as this policy.

3.4 Expectation of Privacy

Norwich University must be positioned to protect critical and sensitive information relating to the privacy of individuals including students, faculty, staff, and contractors, the business of the University and any other information that may accrue to the benefit of the University, its students and its employees.

In order to accomplish this and to comply with state, local and Federal laws, Norwich University retains the right, without advance notice, to inspect computers using the University network and resources, storage media, data in transit over University networks, and data stored in any University or student computer or other computing device. Any interception, inspection, or seizure of a computing device, other information systems device, or data residing on such a device, must have prior authorization by the Vice President of Academic Affairs or his/her designee.

Students and employees of the University may not rely on an expectation of privacy regarding computing systems and data that operate on or have access to Norwich University computing resources.

3.5 Data and Program Damage Disclaimers

Norwich University uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these security measures, the University maintains the authority to:

1. Restrict or revoke any user's privileges with cause.
2. Inspect, copy, remove or otherwise alter any system data, program, or other system resource that may directly impede the protection of confidentiality, integrity, and availability of information.
3. Take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users.

Norwich University disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

3.6 Industry-Specific Information Security Standards

Norwich University information systems must employ industry-specific (i.e., universities and educational institutions) best practices and information security standards. These security standards enable the organization to practice safe security techniques in order to minimize the loss of information and maintain its accessibility and integrity. These guides provide general outlines as well as specific techniques for implementing information security within the university environment.

3.7 Security Testing

Security testing and audit will be performed on all new systems and applications introduced into the University information systems enterprise (“the enterprise”) prior to being placed in production status on the network. Additional testing will be performed on any system or application that has received security-relevant modifications or upgrades prior to that system or application being placed back in production status on the network. This does not include specific audit or testing of student-owned computers except as deemed necessary by the Vice President for Academic Affairs.

Security testing and audit will be performed periodically on the Norwich University enterprise as a whole. This testing may be performed on sections of the enterprise to avoid interruptions to normal operations, but the entire enterprise must be tested for security flaws at least annually.

All security testing/auditing, whether performed by outside contractors or University employees, will follow a test plan approved by the Chief Information Security Officer. Ad hoc testing of individual products and applications prior to being placed into production status may follow a generic test plan. Additionally, all testing will be followed by reports indicating tests performed, results obtained and recommended remediation, if any.

3.8 Incident Response

The University will maintain an active information security incident response plan and will maintain a Computer Incident Response Team. (The Norwich Computer Incident Response Team: N-CIRT). The N-CIRT will be responsible for responding to all incidents, declared as such by the Vice President for Academic Affairs or his/her designee in accordance with the approved incident response plan.

3.9 Policy Non-Enforcement

The University’s failure to enforce any of the requirements of this policy does not constitute consent to violations of the policy nor does it invalidate this policy, any element thereof or standards and practices created under its authority.

3.10 Consequences of Non-Compliance

Non-compliance with information security policies, standards, or procedures is grounds for disciplinary actions up to and including termination or expulsion. Such actions will follow the rules and procedures laid down in the applicable human resources or student policies, standards and procedures.

3.11 Legal Conflicts

Norwich University information security policies are intended to meet or exceed the protections found in existing laws and regulations. Any Norwich University student or employee should report any portion of the information security policy believed to be in conflict with existing laws or regulations to the VPAA.

3.12 Contacting Law Enforcement

Norwich University employees, students and workers must report any information security incidents to a University officer or designee. Every decision about the involvement of law enforcement with information security incidents or problems must be made by the Norwich University Vice President for Academic Affairs (VPAA). Likewise, every direct contact with law enforcement regarding an information security incident or problem must be initiated by an appropriate individual designated by the Vice President for Academic Affairs.

3.13 Disclosure of Information to Law Enforcement

By making use of Norwich University systems, users consent to allow all information they store on Norwich University systems to be divulged to law enforcement at the discretion of the Norwich University Chief Information Security Officer or his/her designee.

3.14 Temporary Accounts

Special users, third party contractors, adjunct instructors, temporary employees, volunteers, or consultants having access to University computing assets, networks, or telecommunications systems should be identified as such in their user names and must follow the same information security rules as University students and employees with the following exceptions:

- Accounts must be deactivated, but not necessarily deleted, at the conclusion of the temporary account users contract
- Temporary account users will be given access only to those University computing resources required to do their jobs

3.15 Viruses and Other Security Incidents

All suspected information security incidents must be reported as quickly as possible to the IT department.

Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. Accordingly, if employees or students report a computer virus infestation to the IT department immediately after it is noticed, even if their negligence was a contributing factor in causing the virus infestation, no disciplinary action will be taken.

The only exception to this early reporting amnesty will be in those circumstances where an employee or student knowingly caused a computer virus to be introduced into Norwich University systems. However, if a report of a known infestation is not promptly made, and if an

investigation reveals that certain employees or students were aware of the infestation but failed to make reasonable efforts to report the problem, these employees or students will be subject to disciplinary action including termination or expulsion consistent with current applicable policies.

Virus checking systems approved by the IT department must be in place on all personal computers with operating systems susceptible to viruses, on all firewalls with external network connections, and on all electronic mail servers that touch the University computing infrastructure. All files coming from external sources must be checked before execution or usage. If encryption or data compression has been used, these processes must be reversed before the virus-checking process takes place. Users must not turn off or disable virus-checking systems.

3.16 Software Development Source

Software that supports production business applications/programs must be either developed in-house, or obtained from a known and reliable third-party vendor. Free software (also known as shareware, freeware or open source software) is not permitted unless specifically evaluated and approved by the Vice President for Academic Affairs or a designee. Such free software is useful and may be an important part of a department's computing or academic infrastructure. Therefore, such approval may not be unreasonably withheld.

3.17 Email Acceptable Use

The Vice President for Academic Affairs with the assistance of the Chief Information Security Officer will establish an email acceptable use standard. This standard will include, but will not be limited to, use of email resources, unacceptable content, procedures for intercepting email when necessary and any other aspects of acceptable email use that are appropriate in support of this Policy.

3.18 Information Security Classification

To assist in the appropriate handling of information, a sensitivity classification hierarchy must be used throughout Norwich University. This hierarchy provides a shorthand way of referring to sensitivity, and can be used to simplify information security decisions and minimize information security costs. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, where it goes, or who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories.

Within one year of the implementation of this policy a standard practice for classifying information within the university must be in place. Within two years of the implementation of this policy the Information Security Classification Standard Practice must be implemented.

3.19 Loss or Disclosure of Sensitive Information

If sensitive information is lost or disclosed to unauthorized parties, or suspected of being lost or disclosed to an unauthorized party, its owner, the Chief Information Security Officer and the appropriate IT personnel must be notified immediately.

3.20 Change Control

Users must not install new or upgraded operating systems or application software on University-owned personal computers or other machines used to process Norwich University information without permission from the University IT Department or an authorized agent. Systems used to process Norwich University information are owned or contracted by Norwich University and have been specifically recognized as systems used for regular organizational activities.

Department managers or other members of the management team may not sign contracts, initiate internal projects, or otherwise make promises that obligate Norwich University to make changes in its computer or communications systems, unless these changes are pre-approved by both the Vice President for Academic Affairs and the Chief Information Security Officer.

3.21 Security Products and Services

All critical information security functions must be supported with best-of-breed, commercially-available products and services.

3.22 Centralized Information Security

Guidance, direction, and authority for information security implementations are centralized for the entire university by Information Technology management under the authority and oversight of the Chief Information Security Officer.