Ohio Supercomputer Center Information Security Framework	**No:** **OSC-3**
	Effective: **05/27/09**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1. Purpose

This policy and its supporting sub-policies provide a foundation for the security of OSC information technology systems. The requirements put forth in this policy and its supporting sub-policies are designed to ensure that due diligence is exercised in the protection of information, systems and services. This policy describes fundamental practices of information security that are to be applied by OSC to ensure that protective measures are implemented and maintained.

2. Scope

Pursuant to Ohio IT Policy ITP-A.1, “Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services,” this policy applies to all systems under the control of the Ohio Supercomputer Center.

The scope of this information technology policy includes OSC computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

3. Background

Security risks associated with information technology are increasing in both number and variety. Information technology network infrastructures are increasingly more complex to implement and administer. The advent of hacking tools and persons willing to distribute viruses and ***malicious code*** has increased the risks to IT organizations and the assets they are charged to safeguard.

OSC functions supported by IT systems continue to expand. Although some ***data*** and systems may not be classified as mission critical, they nevertheless represent a significant investment in resources, contain sensitive data, and are efficient methods of providing a wide range of services. Coupled with overall system integration and interconnectivity, OSC systems and networks are increasingly at risk to intrusions, misuse of data, and other attacks from both internal and external sources.

OSC IT Policy, OSC-3, “Information Security Framework,” is intended as a tool to mitigate increased risks.

A successful security framework is reliant upon strong leadership support and a comprehensive body of effective and efficient information technology security policies and procedures that serve to:

- Promote public trust
- Ensure continuity of services
- Comply with legal requirements
- Recognize risks and ***threats***
- Protect ***system assets***

4. **References**

OSC IT Policy, OSC-3, “Information Security Framework,” is the overarching ***security policy*** for OSC information and services. This policy and its supporting sub-policies should be considered collectively rather than as separate or unrelated policies. The table below illustrates the interrelationship of OSC technology security policies.

Information Security Framework	Security Requirements								
	Risk Management	Confidentiality	Integrity	Availability	Protect, Detect and Respond	Identification & Authentication	Access Control & Authorization	Security Audit Logging	Security Management & Administration
Information Security Framework Policy Sections	5.1	5.2	5.2	5.2	5.3	5.4	5.5	5.6	5.7
SUBPOLICIES									
Business Resumption Planning (E.7)	X			X	X				X
Data Classification (OSU)	X	X	X	X	X	X	X	X	X
Disposal, Servicing and Transfer of IT Equipment	X	X							X
Internet Security	X					X	X		X
Intrusion Prevention and Detection (OSC-12)	X		X		X		X	X	X
Malicious Code Security (OSC-4)	X		X		X				X
Password & PIN Security (OSC-8)	X	X			X	X	X	X	X
Portable Computing Security (OSC-9)	X	X				X	X	X	X
Remote Access Security (OSC-5)	X	X		X		X	X	X	X
Security Education and Awareness (OSC)	X	X	X	X	X	X	X	X	X
Security Incident Response (OSC-7)	X		X	X	X			X	X
Security Notifications (OSC-10)	X	X			X	X	X		X

4.1. Chapter 1306 of the Ohio Revised Code and Rule 123:3-1-01 of the Ohio Administrative Code specifically govern the use of legally binding records and signatures in electronic formats and include companion security requirements to this policy.

4.2. Chapter 1347 of the Ohio Revised Code includes companion security provisions to this policy that require state agencies to, among other things, "take reasonable precautions to protect personal information in the system from unauthorized modification, destruction, use, or disclosure."

4.3. Chapter 149 of the Ohio Revised Code includes companion provisions to this policy with regard to records management requirements and public records requirements. Section 149.433 of the Ohio Revised Code specifically addresses IT security records.

4.4. Ohio IT Bulletin ITB-2007.02, “Data Encryption and Securing Sensitive Data,” effective July 25, 2007, outlines the requirements for the encryption of sensitive data as well as requirements for securing portable devices and media, backups, sensitive data in transmission, and sensitive data at rest. The bulletin also outlines restrictions for sensitive data, physical security considerations, public servant acknowledgement requirements, and incident response.

4.5. Ohio IT Standard ITS-SEC-01, “Data Encryption and Cryptography,” defines minimal requirements for the encryption of sensitive data within state government.

4.6. Ohio IT Standard ITS-NET-01, “802.11 Wireless Local Area Network,” defines minimal requirements for the configuration and use of existing or newly implemented IEEE 802.11 wireless local area networks within state government.

4.7. A glossary of terms for this policy is located in section 9.0 - Definitions. The first occurrence of a defined term is in ***bold italics***.

5. Policy

OSC shall exercise due diligence to ensure that computer and telecommunications systems and services that conduct or support university and state business are secure, and that the information contained within those systems and services is protected from unauthorized disclosure, modification or destruction, whether accidental or intentional.

OSC shall ensure that ***public servants*** are aware of their specific information security responsibilities in the use of state information systems and the handling of information.

The following minimum security requirements provide the foundation for IT security policy development and are described in more detail in this policy. The table in section 4.2 provides a roadmap that illustrates how OSC IT security sub-policies align with the minimum security requirements described below.

- ***Risk Management*****:** OSC shall apply risk management techniques to balance the need for security measures (section 5.1).

- ***Confidentiality*****,** ***Integrity*** and ***Availability*****:** OSC shall ensure ***security policies***, plans and ***procedures*** address the basic security elements of confidentiality, integrity and availability (section 5.2).

- **Protect, Detect and Respond:** OSC security plans and policies shall include methods to protect against, detect, and respond to threats and vulnerabilities to agency information and systems (section 5.3).

- ***Identification and Authentication*****:** OSC shall implement an identification and authentication process for information systems and services (section 5.4).

- **Access Control and *Authorization*:** OSC shall implement access control and authorization policies, plans and procedures as required to protect system assets and other information resources maintained by OSC (section 5.5).

- **Security Audit Logging:** OSC shall implement a security audit logging capability on information systems, including computers and network devices (section 5.6).

- **Security Management and Administration:** OSC shall implement a security management and administration program (section 5.7).

Minimum Security Requirements:

5.1. Risk Management. OSC shall adopt a risk management methodology that incorporates the following risk management processes:

- **Risk Assessment** (section 5.1.1.1) positions OSC to determine effectively the extent of potential threats and the associated risk. The goal of conducting a risk assessment is to identify OSC-specific controls that are appropriate for reducing or eliminating risk;

- ***Risk Mitigation*** (section 5.1.1.2) addresses the prioritization, evaluation and implementation of strategically selected controls. The goal of risk mitigation is to select and implement controls that reduce risk to an acceptable level; and

- **Evaluation and Assessment** (section 5.1.1.3) is a process comprised of activities that recognize and respond to new and changing risks, measure the effectiveness of implemented controls, and modify controls to reflect changes in the three aspects of risk management: operational, technical and managerial. The goal of evaluation and assessment is to maintain a successful and effective risk management program that continuously evolves and responds to changing threats and opportunities.

Risk management offers a practical approach to balancing security with operational requirements and cost. The definition of acceptable risk and the approach to managing risk can vary for each agency. Risk management is a trade-off in which a certain amount of residual risk is accepted as a balance to the costs of incremental countermeasures.

The likelihood that adverse events will occur is determined by analyzing possible threats in conjunction with vulnerabilities and potential business impact. The formula that follows is commonly applied by the information security community to define and measure such risks as a part of risk management. The formula further expresses the relationship of risk exposure factors to counterbalancing security strategies in defining the level of risk:

$$\text{Risk} = \frac{\text{Impact x Threats x Vulnerabilities}}{\text{Countermeasures}}$$ [1]

- Risk factors are defined for each system being measured and receive relative ratings of high (H), medium (M), or low (L).

As an example, risk factor ratings for a hypothetical agency Web server that is linked to patient records might be as follows:

- ***Impact*** – The impact of a successful attack to obtain or change records might be rated as “high.”
- ***Threat*** – The likelihood of an attack might be rated as “medium.”
- ***Vulnerability*** – The system in this example has no protective measures for the server and therefore vulnerability would be rated as “high.”
- ***Countermeasures*** – Alternative measures are robust and therefore would be rated as “high.”

In this hypothetical example, the robustness of the countermeasures may reduce or mitigate the overall risk, resulting in an acceptable level of risk.

5.1.1. OSC risk management practices shall include the elements described in sections 5.1.1.1 through 5.1.1.3 below.

5.1.1.1. Risk Assessment

[1] Randy Nichols, Dan Ryan, and Julie Ryan, Defending Your Digital Assets (New York: McGraw-Hill, 2000) 70.

OSC shall periodically conduct a risk assessment of system assets to address changing threats and organizational priorities. Agency risk assessments shall:

- Identify IT systems, resources and information that constitute each system and prioritize the relative importance of the system assets;
- Identify and document potential threat-sources;
- Identify and document system vulnerabilities that could be exploited;
- Analyze ***security controls*** that have been implemented or are planned for implementation that minimize or eliminate the likelihood of a compromise occurring;
- Determine the likelihood of potential vulnerabilities being exercised by a threat-source;
- Determine the impact associated with the compromise of agency system assets;
- Determine the level of risk using a rating methodology such as high–medium–low;
- Identify technical, operational and management controls that can mitigate or eliminate the identified risks; and
- Document risk assessment results and control recommendations.

5.1.1.2. Risk Mitigation

OSC shall prioritize the implementation of mitigation actions based on the results of the risk assessment. Risks may be eliminated, mitigated, shared with one or more third parties, or accepted. If certain risks are to be eliminated or mitigated OSC shall:

- Evaluate and compare the security countermeasures available, and the resources required to implement them, with the resources required to replace the system assets.
- Determine which countermeasures are reasonable to employ.
- Establish guidelines for implementing management, operational and technical security controls commensurate with the established risk to system assets.

5.1.1.3. Evaluation and Assessment

OSC shall periodically evaluate security controls to determine their ongoing appropriateness and effectiveness for current and anticipated risks and update controls based upon the findings.

5.2. Confidentiality, Integrity and Availability. OSC shall ensure that internal security policies, plans and procedures address the fundamental security elements of confidentiality, integrity and availability. Businesses, citizens and employees expect that sensitive information about them will be shared only with those who need access, that the information will not be altered either by accident or malicious intent, and that it will be available when needed. To this end, OSC shall:

5.2.1. Provide information and services only to those authorized.

5.2.2. Protect information so that it is not altered maliciously or accidentally.

5.2.3. Ensure that information and services are provided in conjunction and accordance with an agency business continuity policy developed in accordance with OSC IT Policy OSC-13, "Business Continuity Planning."

5.3. Protect, Detect and Respond. OSC IT security plans and policies shall include methods to protect against, detect and respond to threats and vulnerabilities. At a minimum, OSC shall:

5.3.1. Determine how much protection is needed and for how long, per the results of the risk assessment outlined in section 5.1, and then develop policies and procedures accordingly.

5.3.2. Review the body of security-related OSC IT policy (see section 4.2) and implement its provisions as required.

5.3.3. Develop a methodology to detect when system assets are safe and when they are threatened. The methodology needs to include auditing and recording the status of all protected system assets at intervals appropriate to the risk as defined in the assessment.

5.3.4. Develop an OSC security incident reporting policy describing how to respond to security incidents that addresses "who," "what," "when," "where" and "how," in accordance with OSC IT Policy OSC-7, "Security Incident Response."

5.4. Identification and Authentication. Based upon the risk assessment, OSC will implement an Identification and Authentication (I&A) process for information systems and services that require controlled access. The identification process shall require the user to present a valid identity using a recognizable method. The most common form of identification is a user ID. The authentication process shall require the user to present verification of identity in a recognizable format. The most common form of authentication is a password. For I&A, OSC shall meet the requirements listed in sections 5.4.1 through 5.4.6 below.

5.4.1. System ***users*** shall have unique and individual user IDs.

5.4.2. User identities shall be validated before issuing user IDs and other credentials. Procedures shall be established for maintaining and managing system user IDs, including procedures for establishing new user accounts, validating existing user accounts, and terminating former user accounts. Inactive user IDs shall be deactivated after a period of no activity, not to exceed six months.

5.4.3. All user credentials shall be protected from unauthorized access and alteration.

5.4.4. A security credentials distribution process shall be developed that ensures the confidentiality, integrity and availability of security credentials such as passwords, PINs, ***biometrics***, tokens and certificates. Password and PIN processes shall fulfill the requirements of OSC IT Policy OSC-8, "Password-PIN Security."

5.4.5. If a user is locked out of a system due to a forgotten password, data entry mistake while entering a password, or any other legitimate error, OSC procedures shall verify valid identification and authentication before permitting access.

5.4.6. An authentication process commensurate with the risk assessment of the system assets shall be established. Robust methods of authentication, such as ***two-factor authentication*** or ***digital certificates***, shall be employed to limit access to systems that contain data requiring more secure access or information whose disclosure would cause serious disruption or harm.

5.5. Access Control and Authorization. OSC shall implement access control and authorization policies, procedures and plans to protect information resources. Access control addresses the securing of systems, both the hardware components and the software components. Authorization addresses the management of permissions to access the various system components, including processes for approving access and restricting access. Restricting access can apply to both invalid users and valid users with limited privileges. To this end, OSC shall:

5.5.1. Secure system assets from physical access by unauthorized persons at all times. At a minimum, system assets shall be in the control of authorized personnel or protected by a locking mechanism.

5.5.2. Manage systems with appropriate access control processes and well-formulated ***access control lists***.

5.5.3. Use the ***least-privilege*** method for granting access to system assets.

5.5.4. Subject all personnel with access to system assets to a ***vetting process*** that is commensurate with the system assets risk assessment.

5.5.5. Ensure that systems can detect and deny unauthorized transaction attempts by any user. Unauthorized attempts shall be logged in accordance with the security audit logging requirements defined in section 5.6.

5.5.6. Implement any restrictions to accessing systems outside of normal working hours.

5.5.7. Ensure that the access control methodology can disable user privileges to those who no longer require access.

5.6. Security Audit Logging. OSC shall implement security audit logging on information systems such as computers, network devices, ***routers***, ***firewalls***, and applications. Audit logging shall be commensurate with the risk assessment findings (see section 5.1.1).

5.6.1. The purpose of audit logging is to maintain a consistent and reliable record of system activity. When properly implemented, audit logging can serve as a preventive measure as well as a forensic aid. A comprehensive record of "who-did-what-when" can discourage asset abuse or be a vital form of evidence to prove culpability or prosecute a perpetrator. OSC shall:

5.6.2. Enable security audit features for system assets and configure them to be sufficient to track attempted security breaches. OSC shall ensure that the audit strategy captures the information necessary to identify who is accessing OSC system assets, access attempts and failures, and violations of security policy. Appropriate processes shall be put in place to review and analyze the logs commensurate with the agency's risk assessment. Audit logs shall be protected from tampering and available for review.

5.6.3. Ensure the confidentiality and security of audit information.

5.6.4. Ensure a separation of duties, where possible, between personnel administering access control functions and those administering security audit logging functions. If these functions cannot be separated, OSC shall document the reasons and develop a process to address conflict of interest concerns.

5.6.5. Ensure that audit logs capture information sufficient to satisfy an inquiry to determine timing, events, impact and ownership of both normal system activity and violations of policy, whether security-related or agency business-related. Based upon a deliberate assessment of the organization, application, information and risk, determine an appropriate data collection scheme and retention schedule for audit logs sufficient to associate specific users with events that breach protocol. If logs are subject to an investigation, they shall be preserved as long as needed.

5.7. Security Management and Administration. OSC shall implement a security management and administration program that ensures cross-functional organizational participation. In addition to developing an information security policy and ensuring security awareness, OSC shall adhere to the requirements presented below in sections 5.7.1 through 5.7.5.

5.7.1. Information Technology Security Management Plan. OSC shall develop, implement and ensure compliance with an agency information technology security management plan. At a minimum, the plan shall:

5.7.1.1. Include the requirements of OSC IT Policy, OSC-3 "Information Security Framework," and each sub-policy.

5.7.1.2. Define methods for the disposal of magnetic and optical media, including the disposal of workstations containing hard drives, OSC IT Policy, OSC-2, "Media Inventory Management."

5.7.1.3. Define methods for the disposal of sensitive information maintained electronically, OSC IT Policy, OSC-2, "Media Inventory Management."

5.7.1.4. Define policies for changes to, deviations from, and waivers of the security management plan.

5.7.1.5. Develop a plan to address systems not in compliance with information security policies and systems at risk of exploitation and compromise.

5.7.2. Security Point of Contact. OSC, in compliance with Ohio IT Policies, shall assign a primary person and an alternate to be responsible for coordinating the information technology security functions within OSC and for implementing the information technology security management plan. General functions of the security point of contact include, at a minimum:

5.7.2.1. Understanding and explaining security requirements.

5.7.2.2. Overseeing security processes and self-assessments.

5.7.2.3. Ensuring implementation of security requirements and process improvement.

5.7.2.4. Ensuring compliance with the Ohio Revised Code, the Ohio Administrative Code, Ohio IT policy, OSU IT policy, agency policies and other federal and state regulations.

5.7.2.5. Implementing security risk management measures.

5.7.2.6. Ensuring timely reporting of information technology security management plans and plan updates.

5.7.2.7. Defining training requirements and ensuring implementation.

5.7.3. ***Security Procedures***. OSC shall ensure that all security procedures are defined, documented and implemented. Affected personnel shall be trained in and shall comply with their respective responsibilities.

5.7.4. ***Security Assessments***. OSC shall establish a process for regular security self-assessments and regularly scheduled independent security assessments.

5.7.5. ***Security Records.*** Ohio Revised Code 149.433 exempts "infrastructure records" and "security records" from Ohio's public records law. OSC shall identify these types of records as defined by ORC 149.433.

6. Procedures

None.

7. Implementation

This policy is effective immediately.

8. Revision History

Date	Description of Change
6/1/2009	Original policy.

9. Definitions

9.1. Access Control List. A list of entities and their authorized access rights to a resource.

9.2 Authorization. A grant to a requesting entity (computer, system, person or process) for access to a protected system and its resources. Not all entities will have access to all state information. Authorization requirements can be implemented using techniques such as access control lists, file and resource permissions, and digital certificates.

9.3 Availability. The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis. Information systems that must ensure availability will likely deploy techniques such as uninterrupted power supplies or system redundancy.

9.4 Biometrics. Biological characteristics such as fingerprint, face or retinal blood vessel patterns used by authentication devices to allow an individual access to information, services or other resources.

9.5 Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could possibly include encryption.

9.6 Data. Coded representation of quantities, objects and actions. The word, “data,” is often used interchangeably with the word, “information,” in common usage and in this policy.

9.7 Digital Certificate. An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be and to provide the receiver with the means to encode a reply.

9.8 Firewall. Either software or a combination of hardware and software that implements security policy governing traffic between two or more networks or network segments. Firewalls are used to protect internal networks, servers and workstations from unauthorized users or processes. Firewalls have various configurations, from stand-alone servers to software on a notebook computer, and must be configured properly to enable protection.

9.9 Identification and Authentication. The verification of the identity of a requesting entity (a person, computer, system or process). Once it is determined who may have access to a system, the identification and authentication (I&A) process helps to enforce access control to the system by verifying the identity of the entity. Systems may use a variety of techniques or combinations of techniques, such as user ID, password, personal identification number, digital certificates, ***security tokens*** or biometrics, to enforce I&A, depending upon the level of access control required to protect a particular system.

9.10 Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act. Because businesses, citizens and governments depend upon the accuracy of data in state databases, agencies must ensure that data is protected from improper change. Information systems that must ensure integrity will likely deploy techniques such as scheduled comparison programs using cryptographic techniques and audits.

9.11 Least-Privilege. A method for assigning privileges in a system. The objective is to assign only those privileges that are necessary to perform the required functions, and ensure that other privileges are not assigned and cannot be improperly accessed. For example, a typical system user should not be assigned rights to read, write and execute all of a department's files when the user only requires the ability to read a subset of these files to do an assigned job.

9.12 Malicious Code. Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.

9.13 Packet. In networking, a packaging unit for transmitting data that has a defined header and data section. The header includes information for routing the packet to the intended destination.

9.14 Packet Filtering. A process that allows or denies an Internet Protocol (IP) ***packet*** based upon criteria in the packet header. Filtering decisions can be based upon the source address of the packet, the destination address, the protocol and the port. Packet filtering is typically implemented on routers or general-purpose computers acting as routers for a network or network segment. Packet filtering is generally effective to control services like Simple Mail Transfer Protocol (SMTP, used for e-mail transmission), Hypertext Transfer Protocol (HTTP, used for Web page transmission) or Network Time Protocol (NTP, used to synchronize time). For services such as Domain Name Service (DNS, which translates names into IP addresses) and File Transfer Protocol (FTP, used to upload files to and download files from the Internet), the more complex security controls available only in proxies may be required.

9.15 Public Servant. Any employee of the state, whether in a temporary or permanent capacity, and any other person performing a government function, including, but not limited to, a consultant, contractor, advisor or a member of a temporary commission.

9.16 Risk Assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security.

9.17 Risk Management. A discipline concerned with the planning, implementing and monitoring of processes for the identification, measurement, control and minimization of security risks to information systems at a level commensurate with the value of the assets to be protected. Risk management attempts to maximize the results of positive events and minimize the results of adverse events.

9.18 Risk Mitigation. A systematic methodology used to reduce risk by employing one of the following risk options: risk assumption, risk avoidance, risk limitation, risk planning, risk transference.

9.19 Router. A network traffic control device that implements network policy and provides a measure of control for traffic entering and leaving a network. Routers help ensure that network traffic reaches its intended destination. During the routing process, routers can implement ***packet filtering*** based on network traffic packet content and discard packets that do not adhere to network policy.

9.20 Security Controls. Management, operational and technical policies, procedures and tools required to achieve and maintain the necessary level of assurance of confidentiality, integrity and availability.

9.21 Security Policy. A written principle or course of action adopted by an agency to ensure that its security affairs are conducted effectively.

9.22 Security Procedure. A method of securely conducting business or of accomplishing a task to ensure security in accordance with established statewide security policies.

9.23 Security Token. A portable, physical device that enables pre-approved access to data or systems. An example is a security-enabled key fob.

9.24 System Assets. Information, hardware, software and services required to support the business of the agency, and identified during the risk assessment process as assets that need to be protected.

9.25 Threat. An event with the potential to cause harm to an information technology process or service. A threat can be natural, human or environmental.

9.26 Two-Factor Authentication. Authentication that incorporates two elements. There are three elements of authentication: “what you know” (for example, a password or PIN), “what you have” (for example, a digital certificate or a smart card), and “what you are” (for example, a biometric). Two-factor authentication is commonly used for access to systems that contain data requiring secure access or information when disclosure would cause serious disruption or harm. It is also known as strong authentication, although strong authentication can have more than two elements.

9.27 Users. For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned computer and telecommunication systems on behalf of the state.

9.28 Vetting Process. A verification process used to validate the identity and trustworthiness of a person who is seeking access to computer systems and networks.

9.29 Vulnerability. A flaw or weakness in system security procedures, design, implementation, or internal controls of business functions supported by technology, processes or facilities which may promote or contribute to a disruption.

10. Related Resources

Document Name
Federal Information Security Management Act of 2002 (Public Law 107-347, Dec. 17, 2002, 116 STAT. 2946)
National Institute of Standards and Technology Special Publication 800-30, “Risk Management Guide for Information Technology Systems.”

11. Inquiries

Direct inquiries about this policy to:

Director of Supercomputer Operations
1224 Kinnear Rd.
Columbus, OH 43212

Telephone: 614-292-9248

OSC IT Policies can be found on the Internet at: www.osc.edu/policies