FACULTY COUNCIL MEETING

**3:00 p.m., Tuesday, December 10, 2019**

# Council Room, 412 Student Union

**AGENDA:**

1. Roll Call

2. Approval of the November 12, 2019 Minutes

3. Approval of Agenda

4. President Hargis – Remarks and Comments

5. Report of Status of Faculty Council Recommendations:

President Hargis, Provost Sandefur and/or Vice Presidents

6. Reports of Liaison Representatives –

1. Emeriti – Barbara Miller

The Emeriti Board will not meet in December and will meet again late January.  The new Web Page for the group is nearly ready and will be up in January. The Emeriti have been asked if new members would be willing to serve on a panel about “Things to know when you retire”, and think this is a good idea and will pursue it.

1. Wellness Center – Kim Beard



1. Women’s Faculty Council – Awilda Rodriguez

The Women's Faculty Council first speaker of the Spring semester will be Dr. Janice Hermann on the OSU food insecurity study. February 5th, 2:30-3:30pm, CLB 106B.







1. Graduate Council – Rebecca Sheehan

*Academic Program Committee.* A variety of degree modifications were approved.

After consideration by the Graduate Faculty at the General and Subject Matter Group meetings this fall, Council took the following actions:

* *Requirement for Advisor Voting in the Affirmative.* Council voted to remove the requirement that the advisor must vote in the affirmative for a passing thesis or dissertation defense.
* *Second Ph.D*. Council voted to not permit pursuing a second Ph.D. degree without preapproval of the dean of the Graduate College prior to the application for admission. Given Ph.D. degrees are research degrees, earning a second Ph.D. degree is highly unusual.

*Graduate Faculty Membership.* Council voted on proposed membership actions voted on by the Subject Matter Groups this fall. Membership actions will be updated in the Graduate Faculty database.

*Role of Non-OSU Faculty Serving on Graduate Committees.* Dean Tucker asked for feedback on the possibility of changing how non-OSU faculty serving on graduate student advisory committees are granted Graduate Faculty status, the length of the designation, and the responsibilities. Currently, non-OSU faculty are given a formal Graduate Faculty status, which is not necessary given that most only serve on specific student committees. Additionally, OSU has no authority over those individuals. This will be a topic for discussion at the Spring Subject Matter Group meetings.

7. Reports of Standing Committees:

a. Academic Standards and Policies: Eric Rebek – No Report

b. Athletics: Justin Talley – No Report

c. Budget: Jam Khojasteh – No Report

d. Campus Facilities, Safety, and Security: Karen Neurohr – No Report

e. Diversity: Justin Moss – No Report

f. Faculty: Matt Lovern – No Report

g. Long-Range Planning and Information Technology: Christopher Crick – Update

19-12-01-LRPIT: Information & Resources Access Control Policy\*

19-12-02-LRPIT Information Security Policy\*

19-12-03-LRPIT Data Stewardship: Data Classification Policy, Responsibilities and Guidelines\*

19-12-04-LRPIT Information Security: Security Awareness\*

h. Research: Dianne McFarlane – No Report

i. Retirement & Fringe Benefits: Griffin Pivateau – No Report

j. Rules and Procedures: Pamela Lovern – No Report

k. Student Affairs and Learning Resources: Toby Nelson – No Report

8. Old Business –

9. New Business –

10. Adjournment

*Refreshments will be served at 2:45 p.m.*

***\*Attached***

**Amended by Passed Failed**

**Recommendation No.** 19-12-01-LRPIT 1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Moved by:**  Long Range Planning & Info. Tech  2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Seconded by:**  3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Passed**         **Tabled**         **Failed**  4.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Title:**    Information & Resources Access Control Policy

**The Faculty Council Recommends to President Hargis that:**

The University adopt the four information security policies requested by the University's Chief Information Officer and developed in consultation with the Council's Long Range Planning and Information Technology committee.

**Rationale:**

Information security policies and procedures are necessary to safeguard sensitive, confidential research and teaching information.  The rights of students, patients and experimental subjects are protected by law, and malicious attacks can expose the university and individual faculty, staff and students to legal and ethical jeopardy.  This action establishes policies, a training program, and a committee with the mandate to monitor and protect against threats to the security of the university's various information systems.

**Oklahoma State University Policy and Procedures**

|  |  |
| --- | --- |
| ***DRAFT***  **INFORMATION & RESOURCES**  **ACCESS CONTROL POLICY** | **Policy Number**  **ADMINISTRATION & FINANCE**  **Information Technology**  **(Month) 2019** |

**PURPOSE**

1.1 With this policy, Oklahoma State University (OSU) sets in general terms the expectations and principles of access control which apply at an institutional level in order to control risk of negative impact on institutional operations due to unauthorized or inappropriate access to University information systems.

**SCOPE**

2.1 This policy applies to all University owned or controlled information technology resources whether individually controlled or shared, stand alone or networked.

2.2. Exceptions may apply for computer systems research and/or teaching or class projects.

2.3 This policy applies to persons, whether students, staff, faculty, or authorized third-party users, within OSU units, colleges, departments and any other affiliated agencies, entities, groups or organizations which at any point, such as in business operations or administrative processes, control University-owned or University-leased information assets or technology resources.

2.4 This policy stipulates basic configurations of and applies equally to all University-owned or University-leased information assets or systems used to access or protect access of those assets.

**DEFINITIONS**

3.1 Data – For the purposes of this document, electronic information (e.g. databases, spreadsheets, email, etc.) or non-electronic (e.g., paper files, publications, hardcopy research, etc.). Information or knowledge concerning a particular fact or circumstance, gained via business operations, academic study, communications, research, instruction, or otherwise, within the pursuit of the University’s mission.

3.2 Data custodian – The authoritative head of the respective College or Department, or a Principle Investigator or Project Director; those who manage and protect data and are responsible for operations relating to the information.

3.3 Data steward – An individual with the responsibility for coordinating the implementation of data classifications through the establishment of definitions of the data sets available for access and the development of policies and/or access procedures for those data sets.

3.4 Information assets – Any University-owned, -leased or -protected information or data.

3.5 Information systems (‘systems’) – Any resource or equipment used for accessing or for controlling access of information assets.

3.6 Information technology resources – Technology and/or computer resources including, but not limited to, personal computers, workstations, mainframes, mobile devices (laptops, tablets, smart phones, etc.), printing equipment, and all associated peripherals and software, and electronic mail accounts, regardless of whether the resource is used for administration, research, teaching or other purposes.

**POLICY**

4.1 Principle of Least Privilege

It is the expectation of OSU that all organizational units will implement a principle of least privilege regarding access control within their college, department, unit or otherwise university affiliated area. The principle of least privilege states that users will receive **no more access than is absolutely required** for that specific user to complete the responsibilities of their position or role within the university.

4.2 Access Control Procedures

1. All organizational units will develop and maintain access procedures specific to the systems under their control.
2. All credentialing for information access (credentials) will be controlled by provisioning and de-provisioning procedures.
3. All access to information systems and all credentials will be role-based, limiting access to only *authorized* (via access procedures) users according to the user’s role within the University.

4.3 Password Complexity

1. Password complexity rules will be applied to all credentialing used to access information systems.
2. Password complexity rules will follow industry standards.
3. Legacy systems which do not allow for industry standard complexity requirements must use the maximum character and complexity allowed by the system.

4.4 Systems Configuration Expectations

1. All systems will be configured with reasonable session timeout rules which will logoff a user, or lock a system, and require re-authorization in order to continue use of the system.
2. All systems will be configured with appropriate audit logging based on data classifications and any state or federal law which would apply to the system audit.

4.5 OSU Network Access Controls

The OSU Information Technology department will secure, regulate, and control University communications via network services which restrict access to University information assets and systems.

Network-based access controls may include, but are not limited to:

1. Restricting remote access to University systems; and
2. Restricting network traffic to or from specific ports, via certain protocols, or when identified as creating excess network burden or otherwise malicious patterns of network usage or behavior.

4.6 Privileged Accounts Access Management

Privileged accounts on information systems determined to be high impact, or otherwise considered critical to the overall functionality of the University’s business structure, will be limited, reviewed, and/or audited to ensure access control integrity.

4.7 Sensitive Data Access

Access to data which is considered Confidential / Regulated (e.g., protected specifically by federal, state, or OSU rules and regulations and includes information which requires protection under contractual agreements) or otherwise which meets the highest level of classification according to any University policies, standards or guidelines regarding data classification must be protected by strong access approval controls, such as, but not limited to:

1. Multi-factor authentication (MFA);
2. Formalized / documented access approvals by appropriate data custodian or steward prior to access provisioning; and
3. Access restrictions as a result of, or tracking, reporting, monitoring, and/or incident response procedures regarding, failed login attempts on University systems.

4.8 Non-Compliance

Non-compliance with this policy can impact the University in a variety of ways, including, but not limited to, breach of sensitive information, government sanctions, loss of accreditation, or hindrance of University business.

Any individual within the scope of this policy:

1. Is expected to report policy violations or other behaviors which constitute non-compliance of this policy to their immediate supervisor or an appropriate authority associated with the related college, department, unit or other affiliated campus organization.
2. If held responsible for a non-compliance violation, can be subject to immediate revocation of privileges to use the University's computing resources and/or University disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

**Amended by Passed Failed**

**Recommendation No.** 19-12-02-LRPIT 1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Moved by:**   Long Range Planning & Info. Tech 2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Seconded by:**  3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Passed**         **Tabled**         **Failed**  4.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Title:**     Information Security Policy

**The Faculty Council Recommends to President Hargis that:**

The University adopt the four information security policies requested by the University's Chief Information Officer and developed in consultation with the Council's Long Range Planning and Information Technology committee.

**Rationale:**

Information security policies and procedures are necessary to safeguard sensitive, confidential research and teaching information.  The rights of students, patients and experimental subjects are protected by law, and malicious attacks can expose the university and individual faculty, staff and students to legal and ethical jeopardy.  This action establishes policies, a training program, and a committee with the mandate to monitor and protect against threats to the security of the university's various information systems.

**Oklahoma State University Policy and Procedures**

|  |  |
| --- | --- |
| ***DRAFT***  **INFORMATION SECURITY POLICY** | **Policy Number**  **ADMINISTRATION & FINANCE**  **Information Technology**  **(Month) 2019** |

**PURPOSE**

1.1 Oklahoma State University (OSU) is committed to protecting the integrity, availability, and confidentiality of sensitive information under University control, complying with legal requirements, and adhering to policies, procedures, standards, and guidelines set by federal and state laws, contractual obligations, the University and Oklahoma A&M System (A&M), or otherwise referenced in this document.

1.2 The purpose of this policy is to recognize OSU’s responsibilities in, and establish mechanisms for, securing information which is electronically transmitted, stored, or processed in pursuit of the institution’s mission.

**SCOPE**

2.1 This policy impacts all employees, staff and faculty of OSU and the Oklahoma A&M System, as well as vendors, contractors, partners, student, collaborators, and any others doing business or research with OSU/A&M.

2.2 This policy applies to certain members of the OSU Information Technology department, the Oklahoma A&M Chief Information Officer, and identified Technology Coordinators or other personnel tasked with management of University information systems.

**DEFINITIONS**

3.1 Information Assets – Any University-owned, -leased or -protected information or data.

3.2 Data – For the purposes of this document, electronic information (e.g. databases, spreadsheets, email, etc.) or non-electronic (e.g., paper files, publications, hardcopy research, etc.). Information or knowledge concerning a particular fact or circumstance, gained via business operations, academic study, communications, research, instruction, or otherwise, within the pursuit of the University’s mission.

3.3 Information technology resources – Technology and/or computer resources including, but not limited to, personal computers, workstations, mainframes, mobile devices (laptops, tablets, smart phones, etc.), printing equipment, and all associated peripherals and software, and electronic mail accounts, regardless of whether the resource is used for administration, research, teaching or other purposes.

3.4 Information systems (‘systems’) – Any resource or equipment used for accessing or for controlling access of information assets.

3.5 User – For the purposes of this document, a person, whether authorized or not, who makes use of, accesses, creates, or alters University information assets or technology resources from any location

**POLICY**

4.1 Information Security Policies

The OSU Information Technology (IT) department will work with users to adhere to applicable policies, procedures, standards, and guidelines associated with securing institutional information, including, but not limited to:

1. Appropriate Use Policy
2. Information Security Awareness
3. Access Control Policy

4.2 Information Security Task Force

The OSU IT department will establish and maintain an Information Security Task Force (‘Task Force’) to address information security, compliance, and governance needs.

1. Task Force Membership

Given the distributed nature of the University’s technology services, the Task Force will be comprised, of but not limited to, the following personnel:

1. Chief Information Officer – Oklahoma State University
2. Chief Information Officer – Agriculture and Mechanical Colleges
3. Information Security Officer and Director of IT Security
4. IT Manager designated for IT Governance, Risk and Compliance
5. Technology Coordinators from each of the following OSU campuses or functional areas:
6. OSU-Center for Health Sciences (OSU-CHS)
7. OSU-Institute of Technology (OSUIT)
8. OSU-Oklahoma City (OSU-OKC)
9. Financial Information Management
10. Human Resources Information Management
11. Institutional Research and Information Management
12. College of Arts and Sciences
13. College of Engineering and Architecture Technology
14. College of Human Sciences and Education, Health and Aviation
15. College of Veterinary Medicine
16. Division of Agricultural Science and Natural Resources
17. Graduate College
18. Edmon Low Library
19. OSU Research
20. Spears School of Business
21. Additional members as required depending on the topic
22. Task Force Operations
23. The Task Force will meet each fall and spring semesters, or as needed depending on identified needs.
24. The Chief Information Officer – OSU will be responsible for scheduling and recording Task Force meetings.
25. The Information Security Task Force’s responsibilities include:
26. Develop policies, general operational procedures, systems configuration or technological process standards, and other IT governance and administrative guidance as needs are identified within Task Force discussions and activities.
27. Provide guidance to Task Force members or the University regarding enforcement of information security policies.
28. As needed or required, in the event of a compromise of information security, the Task Force will assist with and follow applicable and appropriate procedures toward recovering information, mitigating losses, restoring and ensuring data security, and restoring technological services and business operations.
29. Duties of individual members of the Information Security Task Force include:
30. Reporting to the Task Force information security, compliance/regulatory, or governance needs for their campus/area
31. Communicating to students, faculty, staff, or authorized third-parties of policies set by the Task Force.
32. Reporting to the Task Force a need for or actions (which have been or are to be) taken regarding enforcement of information security policies.

4.3 Non-Compliance

Failure to adhere to the security measures referenced in this policy could result in hindered University operations, impaired organizational business, irreparable damage to institutional resources, persons associated with the institution and the community, and/or fines or other government sanctions.

In the event of non-compliance by individuals within the scope of this policy, the University may apply disciplinary procedures including, but not limited to, immediate revocation of user privileges to University information technology resources, revocation of access, required re-training on data security, notification of supervisors, loss of funding, lawsuits, suspension, and possible termination of employment. Further, violations of this policy may result in disciplinary actions including discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

**Amended by Passed Failed**

**Recommendation No.** 19-12-03-LRPIT 1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Moved by:**  Long Range Planning & Info. Tech  2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Seconded by:**  3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Passed**         **Tabled**         **Failed**  4.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Title:**  Data Stewardship: Data Classification Policy, Responsibilities and Guidelines

**The Faculty Council Recommends to President Hargis that:**

The University adopt the four information security policies requested by the University's Chief Information Officer and developed in consultation with the Council's Long Range Planning and Information Technology committee.

**Rationale:**

Information security policies and procedures are necessary to safeguard sensitive, confidential research and teaching information.  The rights of students, patients and experimental subjects are protected by law, and malicious attacks can expose the university and individual faculty, staff and students to legal and ethical jeopardy.  This action establishes policies, a training program, and a committee with the mandate to monitor and protect against threats to the security of the university's various information systems.

**Oklahoma State University Policy and Procedures**

|  |  |
| --- | --- |
| ***DRAFT***  **DATA STEWARDSHIP:**  **DATA CLASSIFICATION POLICY,**  **RESPONSIBILITIES AND GUIDELINES** | **Policy Number**  **ADMINISTRATION & FINANCE**  **Information Technology**  **(Month) 2019** |

**PURPOSE**

1.1 The purpose of this policy is to establish data classification guidelines and minimum requirements to be followed when identifying applicable data and to clarify the data classification responsibilities of data stewards, data custodians, access custodians, and data users.

**SCOPE**

2.1 This policy applies to all data created, collected, stored, processed, or transmitted via institutional resources, in electronic or non-electronic formats.

2.2 This policy applies equally to all University-owned or University-leased information assets and technology resources.

2.3 This policy assigns responsibilities to individuals or individual units within the institution tasked with stewardship, custodianship, or other responsibilities regarding information resources under their control.

2.4 This policy applies to all members of the Oklahoma State University community who have been granted access to University data, whether students, faculty, staff, or authorized third-party users.

**DEFINITIONS**

3.1 Access Custodian – An individual or individuals responsible for implementing the controls identified and/or specified by this policy and the Data Custodian. Appropriate processing, storage, and transmittal protocols of information are under the purview of the Access Custodian.

3.2 Conditions of Use – For the purposes of this document, the restrictions around allowed use of information or data by Data Users or the acceptable circumstances under which Data Users encounter data.

3.3 Data – Information collections, either electronic (e.g. databases, spreadsheets, email, etc.) or non-electronic (e.g., paper files, publications, hardcopy research, etc.). Information or knowledge concerning a particular fact or circumstance, gained via business operations, academic study, communications, research, instruction, or otherwise, within the pursuit of the University’s mission.

3.4Data Custodian – The authoritative head of the respective College or Department, or a Principle Investigator or Project Director; those who manage and protect data and are responsible for operations relating to the information.

3.5 Data Stewards – An individual with the responsibility for coordinating the implementation of this policy through the establishment of definitions of the data sets available for access and the development of policies and/or access procedures for those data sets; or otherwise defined within this document.

3.6 Data User – An individual, whether authorized or not, who makes use of, accesses, creates, or alters information under the scope of this policy.

**POLICY**

4.1 Data Classification

Data for which OSU is to be held responsible shall be assigned one of the following classifications:

Classification Levels

* Confidential / Regulated

Data protected specifically by federal, state, or OSU rules and regulations (e.g. FERPA, Gramm-Leach-Bliley, HIPAA, PCI-DSS, U.S Export Controlled information, Board of Regents policies, etc.) and/or data which includes information which requires protection under contractual agreements (e.g., Non-Disclosure Agreements, various Memoranda of Understanding, Granting or Funding Agency Agreements, etc.).

* Internal

Data available for release under appropriate mechanisms in a controlled and lawful manner.

* Public

Publically available data without requirements for confidentiality, integrity, or availability.

4.2 Classification Expectations

1. Aggregations of information shall be assigned at the highest level of the most restrictive classification requirements of any individual piece of information contained in the aggregate.
2. Social Security Numbers (SSNs) will be treated as Confidential / Regulated data. Security controls for SSNs will include, but not be limited to: authentication for access, masking or encryption for transmission, and encryption for storage.
3. Collection and use of Confidential / Regulated data is only permitted as authorized by law or administrative exception. Data Users will exhibit due diligence to secure collection, storage, processing, or transmission of Confidential / Regulated data. Confidential / Regulated data will not be accessed without legitimate business purpose.

4.3 Personnel Responsibilities

1. Policy Oversight

The highest administrative and financial provisions figure of authority on the OSU campus, such as the Vice President for Administration or Finance or other Vice Presidential position or his/her designee, will have oversight responsibility for:

1. Institutional provisions which define data;
2. Data classification guidelines and standards;
3. Enforcement mechanisms; and
4. Ongoing maintenance of this policy and related explanatory documents.
5. Conditions of Use

Individual units within the institution define ‘conditions of use’ for information resources under their control.

1. These statements must be consistent with this overall policy and may provide additional detail, guidelines, and/or restrictions.
2. Such policies may not relax or subtract from this policy or any institution approved standards.
3. Data Stewards

The Data Steward’s role is to act with proper and appropriate levels of responsibility within a trust relationship regarding institutional data. This role’s responsibilities will reflect OSU’s values regarding both the free exchange of information as an academic institution, as well as a protector of certain information.

1. There will be eight (8) administrative functional areas of OSU, with respective data stewards, as follows:

|  |  |
| --- | --- |
| Administration & Finance | Sr. Vice President for Administration & Finance |
| Admissions/Recruitment | VP Enrollment, Management & Marketing |
| Facilities Management | Chief Facilities Officer |
| Human Resources | Assistant Chief Human Resources Officer |
| Information Technology | Chief Information Officer |
| Research Administration | Vice President for Research |
| Registration/Transcripts | Provost & Sr. Vice President |
| Student Affairs | Vice President for Student Affairs |

1. Data Stewards will be responsible for:
2. Developing access control procedures, in accordance with this University data policy; and
3. Coordinating implementation of the Data Stewardship Policy for administrative areas.
4. Delegation of Data Steward Responsibilities
5. Data Stewards may delegate a portion, but not all, of their Stewardship responsibilities to proper delegates with appropriate levels of operation and/or authority to receive those delegated responsibilities.
6. Delegation of responsibilities does not absolve Stewards of the inherent trust relationship regarding data in which their institutional/operational interests reside.
7. Data Custodians

Data custodians are responsible for:

1. Appropriately classifying data;
2. Ensuring Access Custodians are implementing appropriate and thorough controls for securing data according to the expectations of the data classification level assigned; and
3. Developing means of educating data users on proper security procedures for the data they protect
4. Access Custodians
5. Access custodians are responsible for:
6. Implementing the controls specified by policy, standards, guidelines, and Data Custodians, by administering physical and logical safeguards and monitoring mechanisms for the information resources under their control; and
7. Appropriately and thoroughly educating users of data on the data classification level and expected measures of security associated with that level.
8. May only release data to individuals with a legitimate interest in the data.
9. In certain situations, the roles or responsibilities of Data Steward, Data Custodian, and/or Access Custodian may be held by the same individual.
10. Data Users
11. Data users are responsible for complying with:
    1. All appropriate use policies and procedures; and
    2. All operational requirements associated with this policy.
12. Users who fall within the scope of this policy are responsible for reporting suspected violations of this policy to their immediate supervisor or the institutional department associated with the data involved.

4.4 Appropriate Data Use

Unauthorized access or changes to, or manipulation or release of, data in the following ways are prohibited:

1. Access, manipulate, release, or change of data is authorized if required to fulfill assigned University duties.
2. The individual with the legitimate interest must remain mindful of any University policies or federal, state, or local laws specifically related to the accessing, handling and/or disclosure of that data.

Note: These examples are illustrative, not exhaustive.

1. Do not change data about yourself or others for other than usual business purposes.
2. Do not use information (even if authorized to access it) to support actions by which individuals might profit or benefit (e.g., a change in salary, title, or band level; a better grade in a course).
3. Do not disclose information about individuals without prior supervisor authorization.
4. Do not engage in what might be termed “administrative voyeurism” (e.g., tracking the pattern of salary raises; determining the source and/or destination of telephone calls or Internet protocol addresses; exploring race and ethnicity indicators; looking up grades), unless authorized to conduct such analyses.
5. Do not circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access (e.g., providing a university-wide data set of human resource information to a coworker who only has approved access to a single human resource department), unless authorized.
6. Do not facilitate another's illegal or improper access to OSU’s administrative systems or compromise the integrity of the systems data by sharing your passwords or other information.

4.5 Non-Compliance

Failure to comply with data classification policies and classification standards can result in immediate revocation of privileges to use the University's computing resources, revocation of access, required re-training on data security, notification of supervisors, loss of funding, lawsuits, suspension, and possible termination of employment.

Violations of this policy may result in disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

**PROCEDURAL GUIDANCE**

5.1 Procedural Questions

For questions regarding procedural application of this policy:

|  |  |
| --- | --- |
| **Subject** | **Contact** |
| Policy Clarification | OSU IT Information Security office |

For data stewardship and custodianship specific questions:

|  |  |
| --- | --- |
| **Subject** | **Contact** |
| Administration & Finance | Office of Vice President for Administration & Finance |
| Admissions (Undergrad) | Office of Undergraduate Admissions |
| Admissions (Graduate) | Graduate College |
| Financial Information | Financial Information Management |
| Facilities Management | Facilities Management Administration |
| Human Resources | Human Resources Information Management |
| Institutional Research | Institutional Research & Information Management |
| Information Technology | Office of the CIO |
| International Student Information | International Students & Scholars Office |
| Research Administration | Office of the Vice President of Research |
| Student Information | Office of the Registrar |
| Student Affairs | Office of the Vice President for Student Affairs |

5.2 Regulated Data Chart

This chart is a companion to the policy and provides guidance information on what data may be stored on certain applications. This is not a comprehensive explanation of appropriate use for data; as allowed use is determined by those parties deemed responsible by the policy.

How to interpret the Regulated Data Chart:

**Use Permitted**: No technical, policy, or contractual issues exist that prohibit use of this data type with this service. Sending, storing, or sharing the regulated data type is authorized if the data steward and department/unit policies permit to do so.

******Use Restricted**: Use of this service with the regulated data type is restricted and approval is required.

 **Use Prohibited**: Use of this service with the regulated data type is prohibited. Do not use this service to send, store or share the regulated data type.

| **Application** | **FERPA** | **\*HIPAA (ePHI)** | **Personal Identifiers** | **GLBA** | **Human Subjects** | **PCI** | **Restricted Research Data** | **GDPR** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Email** | | | | | | | | |
| Broadcast Mailing Systems |  |  |  |  |  |  | **** |  |
| Cowboy Mail | **** |  |  |  |  |  | **** | **** |
| Office 365 | **** | **** | **** |  |  |  | **** | **** |
| Orange Mail | **** |  |  |  |  |  | **** | **** |
| **Storage Devices** | | | | | | | | |
| Cowboy Mail SkyDrive | **** | **** | **** |  | **** |  | **** | **** |
| Department Network Drive (G) | **** |  | **** |  | **** |  | **** | **** |
| Orange Mail Google Doc | **** |  | **** |  | **** |  | **** | **** |
| Personal Network Drive (H) | **** | **** | **** |  | **** |  | **** | **** |
| SecureDrive | **** | **** | **** |  | **** |  | **** | **** |
| Sub-Department Network Drive (I) | **** |  | **** |  | **** |  | **** | **** |
| Campus-wide Network Drive (J) |  |  |  |  |  |  |  |  |
| **Document Services** | | | | | | | | |
| Document Imaging | **** | **** | **** | **** | **** |  | **** | **** |
| ePrint | **** | **** | **** |  |  |  |  | **** |
| Remote Printing |  |  |  |  |  |  |  |  |
| **Virtualization** | | | | | | | | |
| Online Classroom Services (D2L, Canvas, etc.) | **** |  |  |  | **** |  | **** | **** |
| Online Classroom Community Sites |  |  |  |  | **** |  | **** |  |
| IT Virtual Labs |  |  |  |  | **** |  | **** |  |
| IT Virtual SAS |  |  |  |  | **** |  | **** |  |
| MSIS Virtual Desktop |  |  |  |  | **** |  | **** |  |
| Real Audio |  |  |  |  | **** |  | **** |  |
| **Support** | | | | | | | | |
| iSupport |  |  |  |  |  |  |  |  |
| TurnItIn |  |  |  |  | **** |  | **** |  |
| **Database Services** | | | | | | | | |
| MS SQL | **** | **** | **** | **** | **** | **** | **** | **** |
| MySQL | **** | **** | **** | **** | **** | **** | **** | **** |
| Oracle | **** | **** | **** | **** | **** | **** | **** | **** |
| **Online Collaboration** | | | | | | | | |
| Drupal |  |  |  |  |  |  | **** |  |
| Omni |  |  |  |  |  |  | **** |  |
| Joomla |  |  |  |  |  |  | **** |  |
| SharePoint | **** | **** | **** |  | **** |  | **** | **** |
| WebDAV |  |  |  |  |  |  | **** |  |
| **Communication** | | | | | | | | |
| Jabber | **** |  |  |  | **** |  | **** | **** |
| MS Lync | **** |  |  |  | **** |  | **** | **** |
| MS Skype | **** |  |  |  | **** |  | **** | **** |
| VOIP Phone Services | **** |  |  |  | **** |  | **** | **** |

* **FERPA** (Family Educational Rights and Privacy Act): Education records. Examples: Class lists, grade rosters, records of advising sessions, grades, financial aid applications.
* **HIPAA** (Health Information Portability and Accountability Act) / **ePHI** (Electronic Protected Health Information): Certain health information. Examples: Health records, patient treatment information, health insurance billing information, health benefits information. \*The OSU A&M Privacy Official and OSU IT Security department must be informed of **any** storage and use of ePHI or “HIPAA data”
* **Personal Identifiers**: Data items which, when stored or used with other information, can identify a unique individual. Examples: Social Security Numbers, driver’s license numbers and bank account numbers.
* **GLBA** (Gramm-Leach-Bliley/Financial Services Modernization Act): Bursar or Financial Aid records.
* **Human Subjects**: Information that reveals or can be associated with the identities of people who serve as research subjects. Examples: names, finger prints, full-face photos, a videotaped conversation or information from a survey filled out by an individual.
* **PCI** (Payment Card Industry): Information dealing with debit, credit, prepaid, e-commerce, ATM, and POS cards. Examples: credit card numbers, names and other information used for payment processing.
* **Restricted Research Data**: Research data sets: Example: Census data and student surveys
* **DMCA** (Digital Millennium Copyright Act): Copyrighted protected material. Examples: audio, video, software, and documents. See OSU *Intellectual Property* Policy 1-0202
* **GDPR** (General Data Protection Regulation): Personal data of EU or European Economic Area citizens or individual personal data transferred from within to outside the EU and EEA areas. Example: an individual EU citizen’s personal data provided to the University

**Amended by Passed Failed**

**Recommendation No.** 19-12-04-LRPIT 1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Moved by:**   Long Range Planning & Info Tech 2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Seconded by:**  3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Passed**         **Tabled**         **Failed**  4.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Title:**    Information Security: Security Awareness

**The Faculty Council Recommends to President Hargis that:**

The University adopt the four information security policies requested by the University's Chief Information Officer and developed in consultation with the Council's Long Range Planning and Information Technology committee.

Rationale:  
  
Information security policies and procedures are necessary to safeguard sensitive, confidential research and teaching information.  The rights of students, patients and experimental subjects are protected by law, and malicious attacks can expose the university and individual faculty, staff and students to legal and ethical jeopardy.  This action establishes policies, a training program, and a committee with the mandate to monitor and protect against threats to the security of the university's various information systems.

**Oklahoma State University Policy and Procedures**

|  |  |
| --- | --- |
| ***DRAFT***  **INFORMATION SECURITY: SECURITY AWARENESS** | **Policy Number**  **ADMINISTRATION & FINANCE**  **Information Technology**  **(Month) 2019** |

**PURPOSE**

1.1 Oklahoma State University (OSU) is committed to educating the user base on cybersecurity threats having the potential to cause harm to the confidentiality, integrity, and availability of organizational data. This policy outlines expectations for an information security awareness program to be followed by faculty, staff, students, and in certain cases, affiliates.

**SCOPE**

2.1 This policy applies to all members of the Oklahoma State University community who have been granted access to University data, whether students, faculty, staff, or affiliates.

**DEFINITIONS**

3.1 Data – For the purposes of this document, electronic information (e.g. databases, spreadsheets, email, etc.) or non-electronic (e.g., paper files, publications, hardcopy research, etc.). Information or knowledge concerning a particular fact or circumstance, gained via business operations, academic study, communications, research, instruction, or otherwise, within the pursuit of the University’s mission.

3.2 Information technology resources – Technology and/or computer resources including, but not limited to, personal computers, workstations, mainframes, mobile devices (laptops, tablets, smart phones, etc.), printing equipment, and all associated peripherals and software, and electronic mail accounts, regardless of whether the resource is used for administration, research, teaching, or other purposes.

3.3 User – For the purposes of this document, a person, whether authorized or not, who makes use of, accesses, creates, or alters University information assets or technology resources from any location.

**POLICY**

4.1 Information Security Awareness Training

Oklahoma State University will provide an Information Security Awareness training program covering common information security issues, which is designed to educate all users within the scope of this policy who access the University’s information technology resources.

1. Training Mandates
2. University employees will be required to complete the Information Security Awareness training program within thirty (30) days of their effective start date.
3. University employees will be required to complete this training program at least every three (3) years.
4. Students will be required to complete the Information Security Awareness training program during their first semester.
5. Administration Responsibilities for Mandates Compliance
6. Department heads are responsible for tracking employee participation.
7. On an annual basis, the OSU Information Technology (IT) department will notify the Human Resources and Provost Offices with relevant employee and student training statuses.
8. The Human Resources department will be responsible for enforcing staff training mandates.
9. The Provost’s Office will be responsible for enforcing student and faculty training mandates.
10. Training records will be retained for a period of no less than three (3) years.

4.2 Training Content and Facilitation

1. It is the responsibility of the OSU IT Department to maintain relevant and up-to-date training material according to campus needs.
2. Campus communications will be used each Fall and Spring semesters to augment the standardized training.
3. Regarding employee participation, the Human Resources standard delivery mechanism for employee training will be utilized.
4. Regarding student participation, the student online course management system will be utilized.

4.3 Non-Compliance

Failure to adhere to the training program as outlined in this policy may result in immediate revocation of privileges to use the University's information technology resources and/or disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.