CLARK ATLANTA UNIVERSITY

Policy 14.3: Information Security Policy

CLARK ATLANTA UNIVERSITY		
Policy and Procedures	**Subject: Information Security Policy**	
Department: OITC	**Review Date:** 12/17/20 **Effective Date:** **01/21/21**	**Issued By:** OITC
Distribution: All University employees	**Required Approval:** University President	**No. of Pages:** **7**
Original Signed by: George T. French, Jr., Ph.D		**Date: 01/21/21**

Policy 14.3 Information Security Policy

Table of Contents

Policy 14.3 Information Security Policy

1.0 Policy Statement

This Information Security Policy defines the minimum guidelines required to protect institutional data and Clark Atlanta University (CAU) information systems from unauthorized access, alteration, or destruction.

2.0 IT Security Principles

- Throughout its lifecycle, all institutional data must be protected in a manner that is appropriate and reasonable based on its level of sensitivity, value, and criticality to the university.

- Any information system that stores, processes, or transmits institutional data shall be secured in a manner that is reasonable and appropriate based on the level of sensitivity, value, and criticality that institutional data has to the university. In cases where university departments, research groups, or third parties require non-Office of Information Technology and Communications (OITC) managed systems to connect to the university network, authorization by the CAU Chief Information Officer (CIO) must be granted prior to connecting.

- Individuals who are authorized to access institutional data shall adhere to the appropriate roles and responsibilities which govern their access.

- Users are individually responsible for any breaches that occur as a direct result of intentional non-compliance to established policy.

- Access to institutional data shall only be granted to authorized users on a need-to-know basis. The Data Steward of any institutional data must approve and verify authorized user access.

- Authorized users shall be informed of the expectations, knowledge, and skills required for protecting institutional data.

- Authorized users must maintain confidentiality of all institutional data, even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.

- Authorized users are responsible for enforcing security controls whenever they place institutional data into non-University-managed devices or services.

- All users' access to University-owned or managed assets will comply with applicable standards, controls, and regulations (e.g. FERPA, HIPAA, GLBA, GDPR, PCI-DSS, Federal Uniform Guidance, etc.).

2.1 Information Access

Physical and electronic access to institutional data must be controlled. The level of control will depend on the classification of the data and the level of risk associated with loss of compromise of the information. The timely removal of user access to systems, services, and accounts (including the return of institutionally owned materials) for employees, affiliates, and contractors is required as per OITC and Human Resources' established IT access procedure for terminated employee. This procedure can be found in the OITC Procedure for Active Directory Domain and Employee Email Account Access, and can be obtained by emailing OITCSecurity@cau.edu.

2.2 Technical Evaluation and Procurement

All technology and software under consideration for purchase must be reviewed by OITC to ensure proper integration into existing infrastructure and applications, as referenced in Clark Atlanta University 7.8.1 Purchasing Policies and Operating Procedures. Any purchases that require processes outside of this Purchasing Policies and Operating Procedures must request an exception as covered in section 3.0 of this policy.

2.3 System Security

All CAU issued systems which connect to the network or handle public and/or institutional data must have OITC-installed and maintained anti-malware protection (where technologically feasible), with scheduled updates.

2.4 External Data Sharing

2.4.1 All sensitive data shared or placed outside the university's control are subject to university policy, and all applicable external regulations and controls. Applicable external regulations and controls include, but are not limited to FERPA, HIPAA, GDPR, PCI-DSS, Federal Uniform Guidance, etc.

2.4.1 All Institutional data transmitted outside the organization require additional safeguards. This includes mechanisms such as email encryption and secure file transfer.

2.4.2 Institutional data governed by regulation must employ the safeguards identified in that established regulation.

2.4.3 Institutional data not governed by regulation requires users to consider additional precautionary measures prior to externally sharing institutional data. This can include:

- Data Stewards determining the appropriateness of external transmission and access to the institutional data.
- Understanding that sharing Protected Health Information (PHI) requires a completed HIPAA Business Associate Agreement unless the communication is authorized for the purpose of treatment, payment, or health care operations.
- OITC review and approval of technical security mechanisms and services for remote access and external transmission of sensitive data.

- Encrypting sensitive data transmitted and exchanged over open networks (such as public internet or outside the university managed network).
    - Email encryption must be employed for all external transmissions of sensitive institutional information.

2.5 Information Integrity Controls

Institutional data must be appropriately safeguarded and employ appropriate security controls to ensure its integrity. Data Custodians must ensure that appropriate physical and technical safeguards are in place to protect the overall integrity of the data under their area of responsibility.

2.6 Mobile Device Security

2.6.1 All personal and University issued mobile devices containing institutional data must be kept in a secure location when not in use, and the device must be access controlled via University implemented controls (i.e. username and password).

2.6.2 Additional requirements may apply for devices traveling outside the U.S. Refer to the University's Export Controls Policy to ensure compliance with these requirements.

2.7 Annual Information Security Awareness Training

All faculty and staff must complete the annual Information Security Awareness Training provided by OITC. This training will serve to instill user security awareness and training on how to protect University resources, and to develop users' skills and knowledge so that they can perform their jobs more securely. The training must be completed within 30 calendar days of assignment.

3.0 Exceptions

Requests for policy exceptions must be submitted in writing to OITC via the Risk Acceptance Form. Those seeking exceptions must complete the form thoroughly identifying reasons why the exception to a policy item is required, compensating controls they intend to employ in lieu of adhering to the policy item, and receive approval from their department/unit head and appropriate signatories. The Risk Acceptance Form can be received by submitting an email requesting the form to OITCSecurity@cau.edu. Once completed, OITC's Technical Director, Executive Director, and IT Security Director will review the request, followed by final review and approval of the CIO.

Additionally, if a department requires IT support that is outside of OITC's normal operating procedures, or what it outlined in this policy, the department may seek to establish an Interagency Memorandum of Understanding (MOU) with OITC. The MOU will serve to review, define, and approve the support and/or processes that are outside of OITC normal operating procedures. It will serve as a formalized agreement for support and expectations from all involved entities. The request to establish an MOU with OITC can be made by emailing

OITCSecurity@cau.edu. . Once completed, OITC's Technical Director, Executive Director, and IT Security Director will review the MOU, followed by final review and approval by the CIO.

Exception requests will be reviewed annually to assess whether the exception needs to remain in place or be revoked. MOUs will be reviewed periodically to assess support and expectations, address required changes, etc.

4.0 Entities Affected by this Policy

This policy applies to staff, faculty, partners, contractors, consultants, temporary, and other workers at Clark Atlanta University, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the University. The use of the university's network and system resources is a privilege, not a right. This privilege can be revoked or amended at the University's sole discretion. Failure to comply with this policy may result in disciplinary action as outlined in established in *Clark Atlanta University's 2.4.0 Code of Ethical Conduct* Policy.

5.0 Definitions

Term	Definition
Institutional data	Any data and information that is owned or licensed by the University.
Sensitive data	Any data and information classified as restricted, also known as confidential, that must be protected against unauthorized disclosure, alteration, or destruction. This includes, but is not limited to: • Personnel files • Student records • Financial records • Institutionally funded research
Data Steward	A Unit Head who, by virtue of their position at CAU, has the authority to appoint data custodians. As such, they have ultimate responsibility for the security, accuracy, and confidentiality of data within their areas of accountability. Data Stewards delegate data management responsibility to Data Custodians (including granting inquiry, entry and update data privileges, and defining business processes.) Data Stewards must review all denials for data access and affirm or override the denial decision prior to user notification.
Data Custodian	The individual designated by the Data Steward to be responsible for management of data. The Data Custodian makes data within their charge available to others for the use and support of the office or department's functions. Before granting access to data, the Data Custodian ensures that protection requirements have been implemented and that a "need to know" is clearly demonstrated. By approving user access to University data, the Data Custodian consents to their use of that data within the normal business functions of administrative and academic offices or departments. Data Custodians are responsible for the accuracy and completeness of data files in their areas, and will revoke users' access privileges should misuse or inappropriate use occur.