Cyber Security Program

Cyber Security Program Goals and Objectives

Goals
- Provide comprehensive Security Education and Awareness to the University community
- Build trust with the University community by being transparent and open with regard to Security initiatives and tools
- Enhance the University’s business processes to ensure consistent security practices are followed
- Anticipate and mitigate risks to the University by proactively monitoring systems and activity throughout the University environment

Objectives

Governance, Risk, and Compliance
- Develop IT Security policies, procedures, and standards, that elevate the security posture of the enterprise, while supporting the business, academic, and research initiatives of the University
- Provide assessments and consultation for business areas governed by regulatory or policy requirements to ensure federal and state laws, industry regulations, and institutional policies are followed
- Develop and manage a Security Awareness and Education curriculum that provides training opportunities, quality materials, and timely communications that empower all members of the University community with the knowledge and skills needed to protect themselves and the University

Security Technology
- Implement and maintain security tools that apply appropriate technical controls for end user devices, and IT infrastructure components, based on their roles and access privileges.
- Ensure security tools are strategically placed within the University environment to defend assets, collect appropriate information, providing monitoring and investigative capabilities of activities on the University network
- Engage with the University community to ensure security standards are followed for application development and systems use

Security Operations
- Develop and implement appropriate monitoring and investigative activities to proactively identify vulnerabilities and respond to cybersecurity events within the University environment
- Follow an organized Incident Response plan to ensure cybersecurity incidents are quickly managed in a consistent manner
- Provide clear and concise communications regarding details of cybersecurity incidents, as well as recovery, and protective measures the University community should follow
Cyber Security Policy

Executive Summary

Clemson University is highly diversified in the information that it collects, processes, and maintains. It is the university’s responsibility to be a good steward and custodian of the information that it has been entrusted, which must be upheld by all members of the university. A strong cyber security program is critical to ensure the university meets this obligation. A key element of the program is a well-defined policy.

The goal of this cyber security policy is to provide guidance and awareness to the university community, ensuring the confidentiality, integrity, and availability of all university technology resources is maintained.

Purpose

The purpose of this policy is to provide awareness and guidance for all faculty, staff, and students to effectively manage risk for the university’s information technology (IT) resources.

Policy Statement

Responsibilities

Cyber Security Authority

Responsibility of Clemson University’s Cyber Security Program belongs to the Chief Information Security Officer (CISO).

The CISO has the responsibility for:

1. Implementation of effective and practical technology, expertise, and processes to secure the network and computing infrastructure of the University.
2. Development and implementation of a security awareness program to be offered periodically to all University faculty, staff and students.
3. Development of a risk assessment procedure to be used for new systems and ongoing monitoring of all existing University systems.
4. Development of global, effective and practical University policies, procedures, guidelines and best practices related to information assurance and security.
5. Creation of incident response procedures to handle instances where University assets are compromised, including problem resolution and appropriate internal/external communications.
6. Has authority to disconnect any device or disable any account if it is believed that either is involved in compromising the information security of the University until such time it
is demonstrated that the device or account no longer poses a threat. Devices will not be disconnected without consultation with agreed upon departmental or unit officials, unless a critical situation exists (i.e., serious vulnerability, denial of service attack, worm or virus attack) and organization officials cannot be contacted quickly.

7. Has authority to stop application development or deployment efforts if it is found during a Risk Assessment that the impact of a particular threat will compromise the information security of the University, until a remedy is implemented to reduce or eliminate the impact of that threat.

8. In exercising this delegated authority, administrative decisions and approvals shall be in accordance with applicable laws, regulations and University policies and procedures.

Users

For the purpose of this policy, the term “Users” shall include all university employees, students, contractors, or visitors with electronic access to university resources.

All users will safeguard their computers, usernames, and passwords by implementing appropriate security measures. No user will allow unauthorized persons access to university data or computing or network resources. All users are responsible for their actions and must take all necessary precautions to ensure that their actions will not affect other university IT resources or users. Security Awareness training is assigned to all users, and must be completed.

No users will knowingly create access into the computing network in such a way as to bypass university security systems.

Safeguarding Data

All data pertaining to student records, university administration, research projects, any Federal or State information, and any other information not explicitly deemed public shall be considered confidential and will be safeguarded by each user having access to that data.

All users should refer to the university’s Data Classification Standards for guidance identifying the appropriate classification of data, and for guidance as to how the data should be stored, processed, and transmitted.

All users will adhere to Federal and State laws concerning privacy. Official releases of data under Freedom of Information requests are to be routed through the appropriate vice-presidential area and/or the Office of General Counsel.

Reporting Incidents

Incident Response is everyone’s responsibility – All university personnel are responsible and accountable for:
• Understanding their responsibilities within the context of an information security or privacy incident.
• Reporting suspected and actual information security or privacy incidents to designated information security and privacy personnel.
• Cooperating with designated information security and privacy personnel in performance of the incident response process.

All users should report suspected security incidents to their local IT support, or by contacting the Cybersecurity team directly at security@clemson.edu

Management of Technology Resources

Network Resources

Clemson Computing and Information Technology (CCIT) is responsible for all planning, implementation, and maintenance of the university computing network. No network devices are to be connected to the network that could potentially cause degradation or disruption of services. All users should contact CCIT at ithelp@clemson.edu for any needs related to network appliances or services.

Systems Administration

All university owned IT resources will be managed by users that understand the university’s IT policies and procedures.

Management of IT resources will be conducted in a professional manner using the following guidelines:

• Services and applications that will not be used must be disabled where practical.
• The most recent security patches must be installed on the system as soon as practical.
  o Documentation and justification of non-compliance to updated patches must be kept and made available when requested.
• Privileged access using root or administrator accounts will only be used when the use of non-privileged accounts is not practical.
• Root and Administrator activity shall be logged or documented
• Where possible an approved system-warning banner should be presented when users access systems.

Event Monitoring

All network devices/appliances, and servers (including virtual) managed by CCIT will be configured to send system, security, and application logs in real time to the CCIT provided log management service.
Disciplinary Sanctions

The university will impose disciplinary sanctions on users who violate the above policy. The severity of the imposed sanctions will be appropriate to the violation and/or any prior discipline issued to that user.

Related Information:
Network Security Policy
Data Classification Standards
Use of IT Resources: Employees
Use of IT Resources: Students
Delegation of Administrative Authority and Responsibility