# Cyber Security Plan

Purpose

Clemson University acknowledges that computing and information technology (IT) are a crucial part of the various aspects of a university and it is for that reason Clemson has prepared this Cyber Security Plan. As a large university, Clemson deals with valuable information and is exposed to numerous threats each day including unauthorized access to Clemson IT systems, data loss or theft, phishing, physical threats such as disaster or destruction of IT resources, and more. To combat these threats, Clemson has a range of technologies, practices, procedures, and policies that are detailed below.

This plan attempts to follow the National Institute of Standards and Technology’s (NIST) Special Publication 800-18, Revision 1 as a baseline for Clemson’s security planning.

Two-Factor Authentication

As part of Clemson University’s continuing commitment to protecting its community of research, faculty, staff and students, the University implemented two-factor authentication for various campus systems, including Canvas throughout 2017.

Two-factor authentication (2FA, for short) asks individuals for a secondary confirmation of their identity at log in using a physical device in their possession (app, text message or phone call). Clemson University will use Duo Security for two-factor authentication.

In order to compel the use of this measure, 2FA is required for a range of crucial apps for both students and faculty. Please see more at CCIT’s page on 2FA [here](https://ccit.clemson.edu/support/faculty-staff/two-factor-authentication/).

Faculty Cyber Security Training

While Clemson has made considerable improvements, cyber-security is continual, ever-changing, and everyone’s responsibility to stay informed. In order to meet this challenge, the University developed an Information Security Awareness Training Course Program, sponsored by CCIT’s Office of Information Security and Privacy, that provides helpful information to address these ever-changing cyber security threats.

Access to the training course programs is provided through the Bridge training system and all University Faculty & Staff are required to complete these courses. The goal is to keep the user community up to date on cyber-security and provide useful information to help protect University data and personal information.

Data Classification

Clemson recognizes the importance of the data that it holds from both its students and employees. Between individuals’ financial information, personal identification information, health information, and more, Clemson is entrusted with important data that it must protect. It is important to be able to evaluate both these data and other more open information like publicly available policies or campus maps to control who can access it.

In order to facilitate this process, Clemson created a Data Classification policy. The purpose of data classification standards is to classify information assets into risk-based categories, which will guide who is allowed to access information and what security precautions must be taken to protect against unauthorized access. The policy can be found [here](https://ccit.clemson.edu/about/policy/cu-it-policies/data-classification/).

Continuous Plan Evaluation

As stated, Clemson recognizes that cyber security is not a static challenge. The nature of cyber threats is constantly changing and it is the responsibility of Clemson to keep up with those changes in order to properly safeguard the data and IT resources of the University. In order to evolve with these changing threats, Clemson ensures that its Cyber Security Policy is not set in stone.

Part of this effort is ensuring that the policy calls for continuous evaluation and review. The Clemson cyber security policy states that the policy must be evaluated at least once a year, but is able to be reviewed at any point. This preserves Clemson’s ability to respond quickly to cyber threats and update its rules accordingly.

Policies, Guidelines, and Standards for Students and Faculty

Clemson also has a range of policies, guidelines, and standards in place regarding everything from acceptable use, passwords and usernames, network security, and more. These policies help provide students and faculty with the knowledge and advice to make smart cyber decisions while protecting the University from threats.

But the existence of these policies is not enough on its own. To make sure that the Clemson community is informed on these topics, Clemson frequently disseminates both internal cyber policies and external information from trusted outside groups. This is done through video series, awareness programs, social media, email campaigns, and more. Reaching out through these different mediums helps broaden the reach of Clemson’s efforts and thus strengthen its cyber security.

Incident Response

All cybersecurity incidents and activity on campus are monitored and acted on via Clemson’s Cyber Security Operations Center (SOC), which is monitored 24/7. This SOC maintains real-time data that is acted on as soon as incidents occur, including monitoring, reporting, remediation of threats, and facilitating improvements to the University’s security posture going forward. The staff of the SOC collaborate with the relevant departments across the University, and strive to provide students with real-world experience in supporting SOC activities in a supervised environment. Having cyber students support SOC activities and learn from what they see in the SOC reinforces important lessons in the student body about cyber awareness and hygiene that in turn enhances the security posture of the University.

In addition to proactive incident response, the Clemson Cyber Security Policy also provides multiple avenues for students and faculty to report suspected cyber incidents. The Clemson cyber security team at security@clemson.edu or the local IT team can be contacted in order to begin the incident response process, collaborate with the SOC and relevant staff of the University, and address these threats as soon as possible.

Physical Security

Threats to information are not limited strictly to those that are online. Clemson recognizes the possibility of unauthorized use via insider threats, whether they are purposeful or accidental. Clemson seeks to provide the best safeguards for practices and procedures for providing controlled physical access to Data Center machine rooms located at ITC and Poole and Agricultural buildings on campus.

To do so, Clemson created the CCIT Data Center Access Policy. The purpose of this policy is to ensure the preservation of Clemson University’s central Information Technology and Computing services, the security of equipment, personnel and the protection of sensitive data. This policy is provided for regulating access to CCIT‟s Information Technology Center and Poole Agriculture Building Data Centers. It is imperative the operational access control be administered to secure these locations. This both keeps out unauthorized users and ensures the behavior of those with access. Those who want access must fill out an application that is then signed by the requestor’s Director or Executive Director and those who do have access risk revocation if they break the rules, are also under constant video surveillance while inside the centers, and must sign in and sign out each time. Clemson takes the privilege of access to these centers very seriously. See the full policy [here](https://ccit.clemson.edu/about/policy/ccit-policies-procedures/data-center-access/).

# Related Information:

[Network Security Policy](https://ccit.clemson.edu/about/policy/ccit-policies-procedures/network-security/)

[CCIT Data Center Access Policy](https://ccit.clemson.edu/about/policy/ccit-policies-procedures/data-center-access/)

[Data Classification Standards](https://ccit.clemson.edu/about/policy/cu-it-policies/data-classification/)

[Two-Factor Authentication with Duo](https://ccit.clemson.edu/support/faculty-staff/two-factor-authentication/)

[Use of IT Resources: Employees](https://ccit.clemson.edu/about/policy/cu-it-policies/use-of-it-resources-employees/)

[Use of IT Resources: Students](https://ccit.clemson.edu/about/policy/cu-it-policies/use-of-it-resources-students/)

[Username and Password Policy](https://ccit.clemson.edu/about/policy/cu-it-policies/usernames-and-passwords/)

[Delegation of Administrative Authority and Responsibility](https://ccit.clemson.edu/about/policy/cu-it-policies/authority-and-responsibility/)

# 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.
	+ 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.

Continuous Evaluation

This policy is subject to continuous evaluation and update by the responsible officer. It will be reviewed at least annually, but can be reviewed and updated at any point to evolve with the changing nature of cyber threats.

# 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](https://ccit.clemson.edu/about/policy/ccit-policies-procedures/network-security/)

[Data Classification Standards](https://ccit.clemson.edu/about/policy/cu-it-policies/data-classification/)

[Use of IT Resources: Employees](https://ccit.clemson.edu/about/policy/cu-it-policies/use-of-it-resources-employees/)

[Use of IT Resources: Students](https://ccit.clemson.edu/about/policy/cu-it-policies/use-of-it-resources-students/)

[Delegation of Administrative Authority and Responsibility](https://ccit.clemson.edu/about/policy/cu-it-policies/authority-and-responsibility/)