Westcliff University Cybersecurity Policy

Westcliff University is committed to maintaining a secure, resilient information technology environment to safeguard and protect its data and resources' confidentiality, integrity, and availability. This cybersecurity policy outlines the principles, responsibilities, and procedures governing the University's cybersecurity program. It is a fundamental component of the university's cybersecurity program and serves as a guide for all members of the university community.

Purpose

This policy sets a framework to protect sensitive information, prevent cybersecurity incidents, follow pertinent laws and regulations and align with U.S. Department of Education guidelines and the U.S. Federal Trade Commission Safeguards Rule, which require:

- Ensuring the security and confidentiality of student information,
- Protecting that information from expected threats or hazards, and
- Protecting against unauthorized access to the information.

Scope

This policy applies to and guides all faculty, staff, students, contractors, and third-party vendors who access, use, or manage Westcliff information systems, data, and technology resources. Users must familiarize themselves with this policy and adhere to its provisions.

Responsibilities

University Leadership

Westcliff leadership, including the Board of Trustees and the Chief Executive Officer (CEO):

- Provide financial and organizational support for the program,
- Approve cybersecurity policies and guidelines, and
- Set an example by following cybersecurity best practices.

Senior Director of Technology

The Senior Director of Technology and Strategy is the University’s Information Security Officer, responsible for:

- Creating, overseeing, and enforcing the University's cybersecurity program,
- Identifying and assessing cybersecurity risks, in liaison with other University departments,
- Testing safeguards regularly for effectiveness,
- Developing, maintaining, and regularly updating and enhancing the University’s information technology infrastructure to enhance effectiveness,
- Classifying data based on sensitivity and applying access safeguards,

- Conducting regular risk assessments to identify, assess, and mitigate risk,
- Ensuring sensitive data is encrypted in transit and at rest, with particular emphasis on the security of student data in transit outside Westcliff's systems,
- Ensuring appropriate staffing, technical, and other resources are allocated for effective cybersecurity,
- Liaising with University departments to ensure references in handbooks and other documents regarding cybersecurity are appropriate and up to date,
- Assessing third-party vendors for their cybersecurity practices and compliance with this policy,
- Reporting cybersecurity risks to senior leadership at least yearly, and more often when justified, and
- Promptly reporting and resolving cybersecurity incidents.

Faculty, Staff, and Students

All members of the Westcliff community must:

- Follow all University cybersecurity policies and guidelines,
- Report all suspicious activity or potential security threats,
- Protect their login credentials and use strong, unique passwords,
- Safeguard sensitive data and follow data classification and handling guidelines,
- Keep their systems and devices up to date with security patches,
- Use University-approved software and tools for University-related activities, and
- Complete regularly scheduled cybersecurity and other IT policy related training.

Information Technology (IT) Department

The Information Technology (IT) Department, under the direction of the Senior Director of Technology and Strategy, is responsible for:

- Managing, maintaining, and upgrading the University's network infrastructure and information systems,
- Implementing technical security controls and measures,
- Patching and updating software and systems to address vulnerabilities,
- Monitoring and filtering network traffic using firewalls and intrusion detection systems,
- Conducting regular vulnerability assessments and security audits,
- Establishing, managing and upgrading an incident alert and reporting plan, and
- Providing technical support and assistance to the University community.

Security Measures

The University must implement, maintain, and upgrade a range of security measures to protect its information and technology assets. Such measures must include restricted, tracked access to server rooms and data centers, and may include:

- Firewalls and intrusion detection systems,
- Anti-malware software and regular scanning,
- Data encryption for sensitive information,

- Access controls and authentication mechanisms,
- Security awareness and training programs, and
- Incident response procedures, and
- Recovery procedures.

Network Security:
Westcliff University's network infrastructure is a critical component of its cybersecurity program. The University hosts nonpublic financial data on Amazon Web Services (AWS), employing robust security measures to ensure data confidentiality and integrity. Additionally, the University operates a campus network monitored and managed by a dedicated network team and network administration staff. Key measures include:

- **AWS Monitoring with New Relic:** Continuous cloud network monitoring is conducted using New Relic to analyze performance, detect anomalies, and manage AWS-hosted resources efficiently.
- **Access Control:** Strict access control policies limit access to authorized personnel only. Access to AWS resources is further restricted by allowing connections exclusively from specific IP addresses.
- **Campus Network Monitoring with Ubiquiti:** The campus network is monitored daily by the network administration team using Ubiquiti tools to detect and respond to unusual traffic patterns or vulnerabilities.
- **Authentication:** Personnel accessing both AWS systems and campus network resources must undergo multi-factor authentication (MFA).
- **Data Encryption:** All sensitive data, whether hosted on AWS or traversing the campus network, is encrypted both in transit and at rest.
- **Traffic Monitoring:** Continuous monitoring of network traffic using intrusion detection/prevention systems (IDS/IPS).
- **Regular Audits:** Routine vulnerability scans, penetration tests, and compliance audits for AWS environments and campus network infrastructure.
- **Incident Response:** A robust process to manage and mitigate network-related incidents promptly.

These measures collectively strengthen the University's ability to safeguard its network and sensitive information against potential cybersecurity threats, ensuring operational resilience and regulatory compliance.

Incident Reporting and Response

The University will maintain an incident response plan to address cybersecurity incidents promptly.

- All suspected or confirmed cybersecurity incidents must be reported immediately to the IT Department and the Director of Technology.
- The University must investigate and mitigate incidents, preserve evidence, and notify stakeholders as required by law.

Compliance

The university must adhere to all relevant federal, state, and local laws and regulations about cybersecurity and data protection including, particularly, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and state-specific data breach notification laws.

Records Retention

Records of cybersecurity policies, procedures, and assessments must be kept for compliance and audit purposes.

Review and Updates

This Cybersecurity Policy will be reviewed yearly, or more often when justified, and updated to address emerging threats and technologies. Policy updates will be communicated to all relevant stakeholders.

Enforcement

Non-compliance with this policy may result in disciplinary action including, for example, termination, academic penalties, or legal action, depending on the severity of the violation.

Assigned Leadership

Senior Director of Technology and Strategy

Related Resources

Federal Trade Commission Safeguards Rule

Compliance with Privacy of Consumer Information Rule of Gramm-Leach-Bliley Act

Update Date

01/05/2025