CAMPUSWORKS



A CAMPUSWORKS GUIDE
FOR COLLEGE PRESIDENTS

Securing Your Institution's Digital Future with NIST's Cybersecurity Framework 2.0

By Byron Sayres

Executive Practice Director, Technology Services

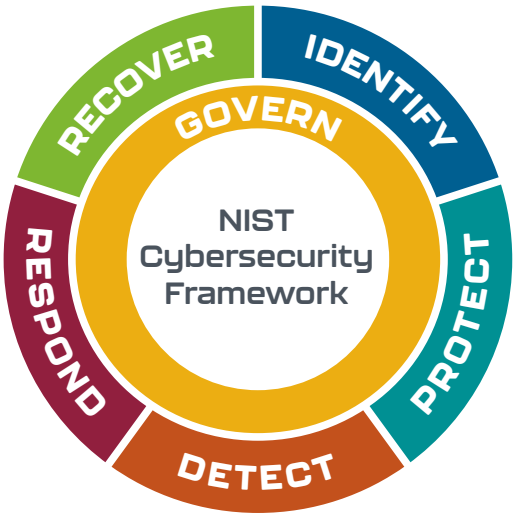
CampusWorks

linkedin.com/in/ByronSayres

As colleges and universities increasingly rely on digital platforms for their day-to-day operations, the release of the National Institute of Standards and Technology's Cybersecurity Framework 2.0 (CSF 2.0) on February 26, 2024, marks a significant step in enhancing cybersecurity measures. This updated framework builds on the solid foundation set by its 2014 predecessor, offering a more comprehensive guide for institutions to bolster their cybersecurity defenses. It stresses resilience and holistic governance, providing a roadmap for educational leaders, especially college presidents, to prioritize and embed cybersecurity into their strategic plans. By fostering a robust cybersecurity culture and ensuring collaboration between presidential leadership and technical teams, institutions can effectively navigate the evolving cybersecurity landscape.

What Leaders Need to Know About NIST's Cybersecurity Framework 2.0

NIST CSF 2.0 integrates a new governance function, affirming its place at the framework's core to establish and oversee a robust cybersecurity risk management strategy. This additional function reinforces the essential role of leadership and governance in cybersecurity.



GOVERN Establish, communicate, and monitor the organization's cybersecurity risk management strategy.

IDENTIFY Understand cybersecurity risks and identify critical assets that need protection.

PROTECT Implement measures to safeguard critical infrastructure and sensitive data.

DETECT Identify cybersecurity events and incidents through the implementation of monitoring and alert systems.

RESPOND Develop a strong response strategy for containing cybersecurity breaches and minimizing damage.

RECOVER Plan and implement recovery strategies to ensure business continuity after a cybersecurity incident.

Next Steps for Implementing NIST's Cybersecurity Framework 2.0

To effectively implement NIST CSF 2.0, we encourage you to take the following strategic actions:

1. **Conduct a Cybersecurity Risk Assessment**—Evaluate your institution's current cybersecurity strategy and posture. Identify necessary adjustments to align with NIST CSF 2.0 and ensure regulatory compliance, including the U.S. Department of Education, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Federal Student Aid (FSA).
2. **Update Cybersecurity Policies and Processes**—Thoroughly review and revise your institution's policies and processes to reflect the comprehensive scope of NIST CSF 2.0. Ensure these updates address all organizational needs beyond just critical infrastructure.
3. **Strengthen Cybersecurity Governance**—Implement the enhanced governance components of NIST CSF 2.0, which include understanding the organizational context, enhancing oversight, developing a risk management strategy, and clarifying roles and responsibilities.
4. **Educate and Train Staff**—Leverage NIST CSF 2.0 as a framework to build a robust cybersecurity culture. Prioritize training for faculty, staff, and students to foster alignment with the framework, emphasizing the importance of governance in cybersecurity.

By prioritizing these steps, you can lead your institution toward a more secure digital future, effectively managing cybersecurity risks in an evolving landscape.

CampusWorks Can Help

CampusWorks' robust portfolio of cybersecurity services can be tailored to your institution's unique needs as you adopt NIST CSF 2.0.



Interim Cybersecurity Leadership

CampusWorks can provide a full- or part-time chief information security officer (CISO) to establish the governance function at the core of your institution's cybersecurity strategy.



Cybersecurity Risk Assessment

CampusWorks will assess your institution's cybersecurity posture, highlighting vulnerabilities to address, policies and processes to update, and action steps required to align with NIST CSF 2.0.



Staff On-Demand

CampusWorks offers technical expertise in network design and architecture, firewall management, and monitoring and alerting, which are essential for safeguarding your institution's critical infrastructure and sensitive data.



Business Continuity Support

CampusWorks' capabilities in cloud, server, and storage management, active directory services, and backup and replication can help detect threats, contain breaches, minimize damage, and ensure business continuity.

Need help securing your institution's digital future? **Let's talk.**

Jon Hazelgren
Vice President of Partnerships
calendly.com/jon-hazelgren

