Dear Presidents,

In 2024, the State University of New York adopted a new and expanded version of Information Security Policy 6900, establishing a system-wide baseline for safeguarding our information assets. This policy formally took effect on September 1, 2025.

As we make this transition, I want to underscore that cybersecurity is not merely a technical concern — it is a leadership imperative and a shared responsibility across every SUNY campus.

Policy 6900 is designed to be both rigorous and adaptable. While it sets a common cybersecurity baseline, it also recognizes that one size does not fit all. For that reason, an exceptions process is built into the policy. This process enables campuses to document where deviations are necessary, ensuring that leadership remains informed and accountable for any residual risk. Campuses are also encouraged to exceed the baseline where their risk assessments indicate it is warranted.

To ensure governance accountability and leadership engagement, SUNY System Administration is requiring each campus to submit an **Annual Information Security Attestation & Risk Statement** by **December 1, 2025**, and annually thereafter.

This requirement is not a compliance audit. Rather, it is a governance measure designed to:

1. **Affirm Executive Accountability** – Campus leaders attest, in writing, to their institution's review of the policy and acceptance of any identified risks.
2. **Enable Risk Management and Resource Alignment** – Campus information security leaders gain a mechanism to communicate and affirm risk acceptance and resourcing decisions.
3. **Provide System Oversight** – System Administration can assess, at a high level, where campuses are excelling or struggling.

The attestation form is intentionally concise and requires a signature from the campus President (or equivalent). Campuses will indicate their implementation status for each major policy domain and acknowledge that responsibility for unmitigated risk rests with campus leadership. Supporting documentation—such as risk assessments, penetration test summaries, or governance committee minutes—may be attached to provide context but is not required or expected.

Completed attestations should be submitted via email to the SUNY CISO, Jesse Sloman (jesse.sloman@suny.edu), no later than **December 1, 2025**. Please work directly with him to arrange alternatives for any supporting documentation that requires more secure handling.

Importantly, the attestation is just one part of SUNY's broader compliance strategy. SUNY System Administration will also assess campus adherence to selected elements of Policy 6900 as part of its annual single audit process. This phased approach allows us to monitor progress, identify gaps, and

direct resources where they are most needed.

Thank you for your continued leadership in protecting SUNY's academic and research mission. Your engagement in this process is vital to ensuring that our campuses remain resilient in the face of today's evolving cyber threat landscape.

Sincerely,
John B. King Jr., J.D., Ed.D.

John B. King Jr., J.D., Ed.D.
Chancellor
The State University of New York
H. Carl McCall SUNY Building
Albany, New York 12246
Tel: 518.320.1355
Twitter | Instagram | Linkedin

Copy: President's assistants