Information Security Policy Attestation – Campus Questionnaire

For compliance with the University Information Security Policy (effective September 1, 2025)

Campus / Entity:	
Submission Date:	

Purpose. This questionnaire affirms campus review of, and compliance with, the Information Security Policy; enables resource alignment by surfacing gaps and exceptions; and provides systemwide oversight.

Section 1: Attestation

I have reviewed SUNY Information Security Policy 6900; verified that we have implemented required controls where indicated and documented exceptions per §3.2.2. I acknowledge that responsibility for any unmitigated risk rests with me and the rest of the campus leadership and that incident-notification thresholds to SUNY System (§5) are understood.

I confirm that the responses in Section 2 accurately reflect the campus's implementation of the Information Security Policy and that items marked Partially Implemented or Planned are supported by time-bound remediation plans or approved exceptions per §3.2.2.

President (or equivalent): _____

(Digital signature field included for convenience, may be signed by hand)

Section 2: Policy Questionnaire

Instructions. For each item, select one status. If a requirement is unmet and in use, an approved exception per §3.2.2 must be on file to be compliant. "Fully Implemented" means all elements explicitly required by the cited section(s) are met.

Status definitions:

Implemented – No Exceptions	Implemented – With Exceptions	Planned	Not Implemented
All required elements met, no exceptions necessary.	Some required elements met; exceptions for unmet requirements documented.	Not yet in place; time-bound plan exists; exceptions documented.	Not yet in place; no plan in place; exceptions may or may not be documented.

A1. Multi-factor authentication *(Policy §6.3)*

- MFA enforced for: (1) remote privileged access, (2) remote network access, (3) VPN, (4) SUNY-federated apps, (5) institutional email.
- Any excluded systems/users have a current, approved exception (e.g., emergency access and service accounts with compensating controls).

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

A2. Endpoint Detection & Response (EDR) *(Policy §11.2)*

- EDR installed on all institutionally-owned desktops/laptops/servers and other EDR-compatible devices.
- *Note: It is expected that most specialized equipment (lab instruments, embedded systems, OT systems and appliances) will not be EDR compatible.*

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

A3. Tamper-proof backups *(Policy §7.3)*

- All backup systems and processes incorporate measures to prevent unauthorized modification or tampering of backed-up data (e.g., immutability, write-once, or equivalent control per platform).
- Control applied to all protected repositories that hold in-scope data.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

A4. Incident response plan & exercise *(Policy §13.1–13.2)*

- A comprehensive IR plan exists and was reviewed within the past 12 months.
- A tabletop exercise occurred within the past 36 months.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

B5. 24×7 monitoring & response *(Policy §11.3)*

- Security alerts are monitored, responded to, and remediated, if necessary, by institutional staff or a third-party service 24 hours a day.
- The sources for security alerts include the following:
    - Alerts generated by one or more centralized log and analysis systems (§11.1, §4.3)
    - EDR (§11.2)
    - Firewalls (§§9.1–9.2)
    - Remote access and/or virtual private network (VPN) tools (§10.3)

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

B6. Vulnerability management *(Policy §12.1–12.3)*

- Documented process includes responsibility assignment, remediation timeframes by severity, tracking progress, verification scans, and exception handling.
- Automated authenticated and unauthenticated vulnerability scans run on a regular basis across network-connected assets

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

B7. Encryption & key management *(Policy §8.1–8.4)*

- Sensitive institutional information, including databases, file servers, backup media, and end-user devices, must be encrypted when stored on any device, system, or storage medium. Sensitive institutional information, including email communications, file transfers, and sensitive web traffic, must be encrypted during transmission over internal and external networks.
- Encryption utilizes current, industry-standard encryption methods and protocols.
- A key-management process exists for the generation, storage, rotation and destruction of keys.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

B8. Access management *(Policy §6.1)*

- The principle of least privilege is enforced through a structured and auditable process for the creation, modification, disablement, and deletion of accounts.
- Periodic reviews are conducted based on risk, access, and behavior, with a particular focus on privileged and service accounts.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

B9. Centralized log management *(Policy §11.1)*

- One or more centralized log aggregation and analysis systems is operational. There are documented procedures for investigating, prioritizing, and escalating alerts based on severity.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

C10. Security awareness training *(Policy §3.3.1)*

- Annual information-security awareness/training is offered to all faculty and staff who access SUNY institution information assets and systems.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

C11. Inventory of critical systems *(Policy §4.3)*

- A current inventory exists of all critical systems whose unavailability would materially impact operations..
- *Note: Institutions are expected to set their own thresholds for determining system criticality.*

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

C12. Vendor risk management *(Policy §4.4)*

- A process exists to assess/manage risks posed by third parties that process/transmit/handle/store institutional information.
- Security requirements appear in contracts/SLAs.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

C13. Cyber insurance *(Policy §3.3.2)*

- Institution maintains cyber breach insurance.
- Where feasible, integral third parties maintain adequate coverage enforced via contract.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

D14. Firewalls *(Policy §9.1–9.3)*

- Edge firewalls provide packet filtering, stateful inspection, threat-feed ingestion, and alerting; deployed per vendor guidance.
- Deviations from vendor-recommended settings and/or configurations are documented with supporting justifications.
- Reviews of firewall policies and rules, with ineffective or deprecated policies and rules removed, completed within the past 12 months.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

D15. Network segmentation *(Policy §10.2)*

- Network segmentation logically separates critical systems and sensitive data according to an implemented plan that defines segmentation technologies, permitted protocols/data flows, and includes periodic architecture reviews.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

E16. ISP documentation *(Policy §3.2.3)*

- A documented Information Security Plan exists and includes the required elements (policy establishment; goals/changes; requirements; risk findings; controls; testing).

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

E17. Risk assessment *(Policy §4.2)*

- One or more risk assessments evaluating threats/vulnerabilities, vendor risks, and risk ratings are used for prioritization of security initiatives.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

E18. Backup testing & recovery *(Policy §7.4)*

- Backups are tested regularly to ensure restoration with minimal disruption.
- There is a defined schedule for testing backups.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

E19. Security metrics & reporting *(Policy §3.2.4)*

- An annual written report on program status, effectiveness, and material risks was delivered to executive leadership within the past 12 months.
- *Note: the interim response report submitted by campuses to the Chancellor earlier this year suffices for this requirement.*

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented

E20. Exception management *(Policy §3.2.2)*

- A risk-based exception process is in place, with annual approvals by the ISP lead and the president/designee.
- The exception documentation includes justification, expected duration, and compensating controls in place.

◯ Implemented - No Exceptions ◯ Implemented – w/Exceptions ◯ Planned ◯ Not Implemented