Intellectual POINT
EXCELLENCE THROUGH EDUCATION

Policies

Student Information System Data Security and Administration Policy

Standards for the Protection, Integrity, and Management of Student Records

Prepared by  Brian L. Lewis-Hardy, SVP, Compliance & Accreditation

Last Updated: July 2025 | Effective August 1, 2025 | Version 25.1

46175 Westlake Drive, Suite 250, Sterling, VA 20165 | Phone: +1 (703) 554-3827 | intellectualpoint.com

Table of Contents

PURPOSE **3**
RESPONSIBLE AUTHORITY **3**
IMPLEMENTATION **3**
APPLICABILITY **3**
EFFECTIVE DATE **3**
POLICY **3**
1. User Access - Authentication 3
2. SIS Administration 3
3. SIS Hosting Services 3
4. Security Policy 4
5. Encryption Policy 5
6. Redundancy Policy 5
7. Backups Policy 6
8. Recovery Policy 6
9. Technical Support 6
EQUIPMENT, REPAIR, AND MAINTENANCE PROVISIONS **6**
BUDGET **7**
REVISIONS **7**
POLICY AVAILABILITY **7**

POLICY CONTENT BEGINS ON NEXT PAGE

PURPOSE	The purpose of this policy is to establish standards for the secure management, access control, and integrity of data housed within the Student Information System (SIS) at Intellectual Point.
RESPONSIBLE AUTHORITY	The Director of Information Technology is responsible for the oversight and enforcement of this policy in coordination with the Registrar and Compliance Officer.
IMPLEMENTATION	Implementation of this policy is carried out by IT personnel, SIS administrators, and designated staff responsible for student records, ensuring compliance with data protection regulations and institutional policies.
APPLICABILITY	This policy applies to all users of the SIS, including academic, administrative, and technical staff who access, manage, or process student data.
EFFECTIVE DATE	**August 1, 2025**

POLICY

1. User Access – Authentication

Passwords include at least 1 number, 1 special character, and 8 to 10 characters. Passwords are NOT rotated to prevent written password logs and exposed passwords. User accounts will deactivate upon 4 consecutive wrong attempts. The user must contact the help desk to request a password reset or reset via an approved email address directly in the portal. A two-factor authentication is required using a secondary device, unless bypassed by the user only when using a browser cookie.

The information contained in the student information system is available to authorized users and students with assigned privileges. Users must login to the system using their unique user and password authentication. All activity in the platform is logged, including failed login attempts.

2. SIS Administration

The SIS administrator is responsible for overseeing the application proper operation, availability, users' administration, backups, security, auditing data, ensuring proper reporting, and content creation.

3. SIS Hosting Services

The SIS is hosted on a robust and reliable infrastructure to ensure continuous availability and performance. The primary hosting is provided by OVH, a leading cloud services

provider known for its high-performance servers and global network. This cloud-based hosting allows for scalability and flexibility to meet the growing needs of our user base.

In addition to the primary cloud hosting, we maintain cold spares on-premise at our main campus data center. These on-premise servers are kept in a standby state and can be activated in the event of a prolonged cloud outage. This hybrid approach ensures that the SIS remains accessible even during extended periods of cloud service disruption, providing an additional layer of reliability.

The on-premise cold spares are regularly updated with the latest system images and data backups to ensure they can be brought online quickly if needed. The decision to activate the on-premise servers is made by the Senior Vice President for Software Engineering in consultation with the technical team, based on the severity and expected duration of the cloud outage.

4. Security Policy

The security of the SIS is paramount, and we employ a multi-layered approach to protect user data and system integrity. Our security policy is built on the principles of least privilege access and zero trust networking.

- **Least Privilege Access**: Users are granted only the minimum level of access necessary to perform their roles. This reduces the risk of unauthorized access to sensitive information or system functions. Access controls are strictly enforced, and user permissions are regularly reviewed and updated as needed.

- **Zero Trust Networking**: This security model assumes no user or device can be trusted by default, even if they are inside the network perimeter. Every access request is verified and authenticated before granting access to resources. This approach minimizes the risk of internal threats and lateral movement by attackers within the network.

In addition to these principles, we implement robust firewalls, intrusion detection and prevention systems, and regular security audits to identify and mitigate potential vulnerabilities. All API and network traffic is monitored for suspicious activity, and any anomalies are promptly investigated by our security team.

User authentication is a critical component of our security policy, requiring strong passwords to ensure that only authorized users can access the system. Regular security training is conducted for all staff and faculty to maintain awareness of best practices.

5. Encryption Policy

Data encryption is a fundamental aspect of our security strategy, protecting sensitive information both in transit and at rest.

Data in Transit: All communications between users and the SIS are encrypted using Transport Layer Security (TLS) version 1.2 or higher. This ensures that data cannot be intercepted or tampered with during transmission. We enforce the use of TLS 1.2 for all API interactions, providing a secure channel for data exchange.

Data at Rest:

- Blob and object storage are encrypted using Server-Side Encryption with Object-Managed Keys (SSE-OMK), ensuring that each object is encrypted with a unique key managed by the storage service.

- In our databases, sensitive fields such as personal identification information, financial data, and authentication credentials are encrypted using the Advanced Encryption Standard (AES) with 256-bit keys. This provides a high level of protection against unauthorized access, even in the unlikely event of a database breach.

Encryption keys are managed securely, with access restricted to authorized personnel only. Keys are rotated regularly, and all key management activities are logged and audited.

6. Redundancy Policy

To ensure high availability and resilience against failures, the SIS infrastructure incorporates redundancy at multiple levels.

- **Primary/Core API Services**: These services are deployed in an active-active-passive configuration. This setup includes two active instances running in the cloud on OVH, providing load balancing and immediate failover capabilities. A passive (cold spare) instance is maintained on-premise, which can be activated if both cloud instances become unavailable.

- **Secondary/Internal Tools**: These tools are deployed in an active-passive setup, with one active instance in the cloud and a passive instance on-premise. If the cloud instance fails, the on-premise instance can be brought online manually to ensure continuity of service.

Regular tests are conducted to verify the effectiveness of the failover mechanisms and to ensure that all components can be quickly restored if needed.

7. Backups Policy

Regular backups are essential to protect against data loss and ensure business continuity. Our backups policy provides comprehensive coverage for all critical data and services.

- **Core Services**: Backups are taken twice daily at 6 PM and 5 AM, capturing a complete snapshot of the system to ensure recovery to a recent state.
- **Secondary Services**: Backups are taken weekly, as these services are less critical to daily operations.

All backups are encrypted and stored in a multi-region replicated object storage system to ensure availability. The latest backup is also stored on-premise in the cold-spare databases and as flat files for additional redundancy. Backups are retained for at least one year, supporting operational recovery and compliance requirements. Quarterly tests verify backup integrity and restoration processes.

8. Recovery Policy

In the event of a system failure or disruption, our recovery policy ensures that the SIS can be restored quickly with minimal impact to users.

- **Core Services**: Automatic failover mechanisms allow seamless failover between active instances in the cloud. If both cloud instances fail, the on-premise cold spare can be activated by the technical team.
- **Secondary Services**: Manual intervention is required to switch to the on-premise instance. The technical team will assess and initiate the failover process, switching back to cloud services once restored.

Detailed recovery procedures are documented and regularly reviewed, with staff trained for swift response. Data restoration uses the most recent backup, targeting a recovery time objective (RTO) of 2 hours for core services and 4 hours for secondary services. Regular drills ensure systems can be restored within these RTOs.

9. Technical Support

Technical support is available 24×7 everyday of the year for students, staff, and faculty, through the platform directly, or via email at support@intellectualpoint.com, or by calling (855) 590–3718. Response time: <24h.

EQUIPMENT, REPAIR, AND MAINTENANCE PROVISIONS

The equipment necessary for the implementation of this policy is the responsibility of the Senior Vice President for Software Engineering, who coordinates any repairs, purchases, or

updates required. Such requests are to be made directly to the Senior Vice President of Software Engineering via email, who will follow up accordingly.

BUDGET

The funding necessary for the implementation of this policy is allocated in the institution's annual operating budget under the line item "Technical Infrastructure." Revisions to the funding need approval by the Chief Financial Officer.

REVISIONS

Revisions to this policy are to be approved at one of the Institutional Assessment and Improvement meetings. Personnel is informed of revisions via email. Revisions are published at the staff and student webpage.

POLICY AVAILABILITY

Intellectual Point's policies and procedures are available for review by administrative staff, faculty, advisory members, and students at https://compliance.intellectualpoint.com.