POLICY 3.6 – Data Security Policy

POLICY SECTION:	**Administrative – Information Technology**
RELATED BOARD POLICY:	**1.4.6 Records Management**
RELEVANT LEGISLATION:	**N/A**
PRIMARY APPROVER:	**President**
SECONDARY APPROVER:	
RESPONSIBLE AUTHORITY:	**Institutional Planning and Analysis Committee**
DATE APPROVED:	
DATE(S) REVIEWED / REVISED:	
POLICY REVIEW - FREQUENCY:	**To be reviewed every 3 years.**
APPROVER SIGNATURE(S):	

1. Purpose The purpose of this Data Security Policy is to establish guidelines for protecting the confidentiality, integrity, and availability of King's data assets. This policy ensures compliance with legal, regulatory, and institutional requirements, and supports the University's strategic objectives.

2. Scope This policy applies to all University data, IT systems, and infrastructure, including data stored, processed, or transmitted by faculty, staff, students, contractors, and third-party service providers. It covers data in any format, including electronic, paper, and cloud-based storage.

3. Data Security Principles

3.1 Confidentiality Ensuring that sensitive data is accessed only by authorized individuals and protected from unauthorized disclosure.

3.2 Integrity Maintaining the accuracy and reliability of data throughout its lifecycle by preventing unauthorized modifications.

3.3 Availability Ensuring that data is accessible when needed by authorized users, with minimal disruptions.

4. Data Classification and Protection Data shall be handled according to the King's Data Classification Policy, which categorizes data as Confidential, Private, or Public. Security measures shall be applied according to these classifications:

4.1 Confidential Data Security

- Access restricted to authorized personnel only.
- Data encryption for storage and transmission.
- Multi-factor authentication (MFA) required.
- Regular audits and monitoring.

4.2 Private Data Security

- Access limited to approved University personnel.
- Secure storage and transmission protocols.
- Role-based access control (RBAC) applied.

4.3 Public Data Security

- No special access restrictions.
- Regular review to ensure accuracy and relevance.
- Public access logging.

5. Data Privacy Data privacy shall be governed by King's Privacy Policy. All personnel must adhere to privacy regulations, including compliance with all applicable legislation including FIPPA & PHIPA, ensuring that personal data is processed lawfully and securely.

6. Incident Response

6.1 Incident Reporting All data security incidents, such as breaches, unauthorized access, or data loss, must be reported immediately to the University's IT Security Team and/or the Privacy Officer. The IT Security Team and/or the Privacy Officer will inform the appropriate data owner.

6.2 Incident Response Process The University shall follow a structured incident response process, including:

- Identification: Detect and verify the incident.
- Containment: Limit the impact of the incident.
- Eradication: Remove the cause of the incident.
- Recovery: Restore affected systems and data.
- Lessons Learned: Conduct post-incident reviews and improve security measures.

7. Roles and Responsibilities

7.1 Institutional Planning & Analysis Committee (IPAC)

- Provide oversight and strategic direction for data security.
- Ensure alignment with institutional goals.

7.2 Data Officer

- Oversee implementation of data security controls.
- Allocate resources for security initiatives.

7.3 Data Owners

- Ensure appropriate security measures are applied to their data.
- Approve access and oversee compliance.

7.4 Data Stewards

- Enforce security policies within their data domains.
- Monitor compliance and report incidents.

7.5 Data Custodians

- Implement technical security measures.
- Maintain logs and audit trails.

7.6 Data Users

- Adhere to security policies and report incidents.
- Ensure safe handling of data.

8. Security Controls

- Firewalls and intrusion detection/prevention systems.
- Data encryption in transit and at rest.
- Regular security audits and vulnerability assessments.
- Security awareness training for all personnel.
- Data literacy and security awareness training programs to educate users on best practices and responsibilities.

9. Compliance and Enforcement Failure to comply with this policy may result in disciplinary action up to and including termination, including loss of access privileges and legal consequences.

10. Review and Updates This policy will be reviewed triennially by the Institutional Planning & Analysis Committee (IPAC) to adapt to emerging threats and regulatory changes.

11. Contact Information For questions or concerns regarding this policy, please contact the Institutional Planning & Analysis Committee at IPAC@kings.uwo.ca.