POLICY 3.5 – Data Classification 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 Classification Policy is to establish a framework for classifying King's data based on its sensitivity and criticality. Proper classification ensures appropriate handling, access, and protection of data to comply with regulatory, legal, and institutional requirements.

2. Scope This policy applies to all institutional data created, collected, stored, processed, or shared by faculty, staff, students, contractors, and third-party service providers. It covers all data in any format, including electronic, paper, and cloud-based storage.

3. Data Classification Levels King's University data is classified into three levels based on sensitivity and the potential impact of unauthorized disclosure, modification, or loss.

3.1 Confidential Data

- **Definition:** Data that, if disclosed, could cause significant harm to individuals, the University, or its affiliates. Access to this data is strictly limited.
- **Examples:**
  - Personally Identifiable Information (PII) such as Social Insurance Numbers (SIN), financial account details, and medical records.
  - Prospect, inquiry, applicant, student, and alumni records protected under FIPPA and PHIPA.
  - Research data subject to confidentiality agreements.
  - Human resources records, including payroll and performance evaluations.
  - Legal and contractual documents.

- **Handling Requirements:**
  - Encryption must be used for storage and transmission.
  - Access is limited to authorized personnel with a legitimate need-to-know basis.
  - Physical and logical access controls must be implemented.
  - Data must be securely disposed of when no longer needed.

3.2 Private Data

- **Definition:** Data that, while not classified as confidential, requires protection due to regulatory, ethical, or business considerations.
- **Examples:**
  - Internal University communications.
  - Non-public financial reports.
  - Donor and alumni contact information.
  - Proprietary business process documentation.
- **Handling Requirements:**
  - Access should be limited to authorized users.
  - Data should not be shared externally without proper authorization.
  - Secure methods should be used for storage and transmission.
  - Data must be reviewed periodically for relevance and retention.

3.3 Public Data

- **Definition:** Data that is intended for public dissemination and does not require special handling.
- **Examples:**
  - Published research findings.
  - Marketing and promotional materials.
  - Course catalogs and schedules.
  - University website content.
  - Press releases and public reports.
- **Handling Requirements:**
  - No access restrictions are required.
  - Data must be reviewed periodically to ensure accuracy and relevance.
  - Public data should be clearly marked as such.

4. Responsibilities

4.1 Data Owners

- Responsible for classifying data within their domain and ensuring compliance with this policy.
- Approve access and ensure proper controls are in place (including access audits).

4.2 Data Stewards

- Implement classification guidelines and oversee data handling procedures.
- Monitor data usage and report any breaches or misclassifications.

4.3 Data Custodians

- Ensure technical security measures align with data classification levels.
- Implement data protection measures such as encryption and access controls.

4.4 Data Users

- Understand and adhere to the data classification policy.
- Report any unauthorized access or mishandling of data.

5. Enforcement Violations of this policy may result in disciplinary action including termination in accordance with King's policies and procedures, including loss of access privileges and potential legal action.

6. Review and Updates This policy will be reviewed triennially by the Institutional Planning & Analysis Committee (IPAC) to ensure it remains aligned with evolving regulatory and security requirements.

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