POLICIES AND PRACTICES OF THE COLLEGE

# POLICY 3.4 – Data Access Control 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 Access Control Policy is to establish guidelines for managing and controlling access to King's University data and IT resources based on data classification levels. This policy aims to ensure the confidentiality, integrity, and availability of institutional data while aligning with regulatory, legal, and institutional requirements.

**2. Scope** This policy applies to all University personnel, including faculty, staff, students, contractors, and third-party service providers who access University data and IT systems. It covers all institutional data as classified in the King's Data Classification Policy.

## 3. Access Control Principles

**3.1 Least Privilege Principle** Access to data and IT systems shall be granted based on the minimum level of access required for users to perform their role's functions.

**3.2 Need-to-Know Principle** Access shall only be granted to users who have a legitimate need to access specific data, ensuring appropriate handling and security.

**3.3 Role-Based Access Control (RBAC)** Access permissions shall be assigned based on user roles within the University, ensuring consistency and reducing the risk of unauthorized access.

**3.4 Separation of Duties** Critical tasks and data handling responsibilities shall be distributed among multiple individuals to prevent fraud or errors.

**4. Access Control Levels** Access to university data shall be granted based on the classifications defined in the King's Data Classification Policy:

### 4.1 Confidential Data Access

- **Access Restrictions:**
  - Restricted to authorized personnel only.
  - Requires approval from Data Owners.
  - Multi-factor authentication (MFA) must be enforced.
  - Encryption must be used for storage and transmission.
- **Examples:** Financial records, PII, student records.

### 4.2 Private Data Access

- **Access Restrictions:**
  - Limited to authorized University personnel.
  - Requires approval from Data Stewards.
  - Secure transmission protocols must be used.
- **Examples:** Internal reports, donor information.

### 4.3 Public Data Access

- **Access Restrictions:**
  - Open access with no authentication required.
  - Data must be reviewed periodically to ensure accuracy.
- **Examples:** Marketing materials, course catalogs.

## 5. Roles and Responsibilities

### 5.1 Institutional Planning & Analysis Committee (IPAC)

- Oversee access control policies and ensure alignment with institutional goals.
- Approve access control frameworks and guidelines.

### 5.2 Data Officer

- Provide strategic leadership and resources for access control implementation.
- Ensure IT infrastructure aligns with access control objectives.

### 5.3 Data Owners

- Approve access requests based on the classification of data.
- Ensure access controls align with business and security requirements.

### 5.4 Data Stewards

- Manage access permissions within their respective data domains.

- Monitor access and report any discrepancies or unauthorized attempts.

### 5.5 Data Custodians

- Implement technical controls to enforce access policies.
- Maintain logs and audit trails of data access.

### 5.6 Data Users

- Adhere to access control policies and guidelines.
- Report any unauthorized access or security concerns.

## 6. Access Request and Approval Process

- Users must submit access requests through the designated University access management system(s). (i.e., Service Request Ticket to ITS)
- Requests must be approved by the appropriate Data Owner or Steward.
- Periodic access reviews will be conducted to ensure compliance with the principle of least privilege.

## 7. Authentication and Authorization

- All users must authenticate using strong password policies and MFA where applicable.
- Authorization shall be based on role assignments and classification levels.
- Access privileges will be automatically revoked upon termination of employment or changes in roles.

## 8. Monitoring and Auditing

- Systems will be designed to ensure that access logs and change logs are auditable. Regular audits of access logs will be conducted to detect anomalies and unauthorized access.
- Automated tools shall be used to monitor access and flag potential security risks.
- Users found in violation of the policy will be subject to disciplinary action.

## 9. Enforcement and Compliance

- Violations of this policy may result in the revocation of access privileges or disciplinary action up to and including termination.
- The University reserves the right to monitor and review data access to ensure compliance with this policy.

**10. Review and Updates** This policy will be reviewed triennially by the Institutional Planning & Analysis Committee (IPAC) to align with evolving security and regulatory requirements.

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