# International Balkan University (IBU)
# Information Security Policy

The Information Security Policy establishes guidelines for protecting the university's information assets against unauthorized access, disclosure, alteration, and destruction. This policy is designed to ensure the confidentiality, integrity, and availability of information resources in compliance with legal and regulatory requirements.

This policy applies to all university employees, faculty, staff, students, contractors, vendors, and other users with access to the university's information systems, data, and resources. It covers all forms of information, including electronic, physical, and cloud-based data.

1. **Information Security Objectives**
   The university's information security objectives include:
   - **Confidentiality**: Ensuring that sensitive and personal information is accessible only to authorized individuals and entities.
   - **Integrity**: Protecting information from unauthorized modification or corruption to maintain accuracy and reliability.
   - **Availability**: Ensuring information and resources are available to authorized users when needed.
2. **Roles and Responsibilities**
   - **Information Security Officer (ISO):** The ISO is responsible for developing, implementing, and overseeing the university's information security program. The ISO ensures compliance with security policies and responds to security incidents.
   - **Data Owners**: Data owners are individuals or departments responsible for managing and protecting specific data. They define access rights and ensure that appropriate security measures are implemented.
   - **System Administrators**: System administrators are responsible for implementing security controls on systems, networks, and applications under university policies.
   - **Users**: All users of university information systems are responsible for following the security policies and practices outlined in this policy. Users must protect their accounts, report security incidents, and adhere to acceptable use guidelines.
3. **Access Control**
   - **Authentication**: Access to university information systems requires unique usernames and strong passwords. Multi-factor authentication (MFA) is required to access sensitive systems and data.
   - **Authorization**: Access to data and systems is granted based on the principle of least privilege, ensuring that users have only the minimum access necessary to perform their job functions. Role-based access control (RBAC) enforces this principle.
   - **Account Management**: User accounts must be created, managed, and deactivated

according to defined processes. Former employees' or students' accounts must be promptly deactivated to prevent unauthorized access.

- **Periodic Review**: Access rights must be reviewed periodically to ensure they are still appropriate. Data owners and system administrators must regularly audit access permissions.

4. **Data Protection**
    - **Data Classification**: University data must be classified as public, internal, confidential, and sensitive. Each classification level has specific handling requirements that must be followed to protect the data.
    - **Encryption**: Sensitive data must be encrypted both at rest and in transit. This includes data stored on servers, databases, laptops, and mobile devices and transmitted over networks.
    - **Data Backup**: Critical data must be regularly backed up and securely stored. Backup procedures must be documented, and backups must be tested periodically to ensure data can be restored during a failure or disaster.
    - **Data Retention and Disposal**: Data must be retained under the university's Data Protection Policy and legal requirements. When data is no longer needed, it must be securely disposed of, including deleting electronic records and shredding physical documents.
5. **Network Security**
    - **Firewalls and Intrusion Prevention**: The university's network must be protected by firewalls and intrusion prevention systems (IPS) to detect and block unauthorized access and malicious activities.
    - **Network Segmentation**: Critical systems and sensitive data should be segmented from general network traffic to reduce the risk of compromise. Segregated networks must be used for guest access, student Wi-Fi, and other non-critical systems.
    - **Wireless Security**: Wireless networks must be secured using robust encryption protocols (e.g., WPA3) and authentication measures. Unauthorized wireless access points (APs) are prohibited, and personal Wi-Fi devices on university premises must be regulated.
6. **Endpoint Security**
    - **Antivirus and Anti-malware**: All university-owned devices and any personal devices connected to the university network must have up-to-date antivirus and anti-malware software installed and configured for regular scans.
    - **Device Encryption**: Laptops, mobile devices, and external storage devices that store sensitive data must be encrypted to prevent unauthorized access in case of theft or loss.
    - **Patch Management**: All systems and devices must be updated with the latest security patches. Critical security updates must be applied as soon as possible, and system administrators must regularly review and manage patching activities.
7. **Incident Management**
    - **Incident Reporting**: All users must report security incidents, such as data

breaches, unauthorized access, or malware infections, to the Information Security Officer immediately. The university's incident reporting procedure must be followed to ensure timely response and mitigation.

- **Incident Response Plan:** The university maintains an incident response plan outlining the steps to be taken in case of a security breach or other incident. This plan includes containment, eradication, recovery, and communication procedures.
- **Post-Incident Review**: After a security incident, a post-incident review must determine the root cause, assess the impact, and implement corrective actions to prevent future incidents.

**8. Security Awareness and Training**

- **Employee Training**: All employees, faculty, and staff must complete mandatory security awareness training upon joining the university and at regular intervals. Training covers key security topics such as phishing, password management, and data protection.
- **Student Awareness**: Students must be aware of their information security responsibilities through orientation programs, periodic awareness campaigns, and access to security resources.
- **Ongoing Awareness**: The university will regularly conduct awareness campaigns and distribute security tips to inform the community about emerging threats and best practices.

**9. Third-Party and Vendor Management**

- **Vendor Security Requirements**: Third-party vendors and service providers who handle university data or access university systems must comply with the university's security policies. Data processing agreements (DPAs) must be established to outline security requirements and responsibilities.
- **Due Diligence**: The university must conduct due diligence assessments of third-party vendors to evaluate their security practices before engaging in any data-sharing or service provision.
- **Monitoring and Auditing**: Third-party vendors must be monitored and audited to ensure compliance with the university's security requirements. Non-compliance may result in the termination of contracts and access.

**10. Compliance and Auditing**

- **Regulatory Compliance**: The university must comply with all applicable laws, regulations, and industry standards regarding information security, including GDPR, FERPA, HIPAA (if applicable), and PCI-DSS.
- **Internal Audits**: Regular internal audits must be conducted to assess compliance with security policies and identify areas for improvement. Audit findings must be documented, and corrective actions must be implemented promptly.
- **External Audits**: The university may be subject to external audits by regulatory bodies or third-party assessors to ensure compliance with security requirements. Cooperation with external auditors is mandatory.

**11. Policy Review and Updates**

- The Information Security Officer will review this policy annually and update it as

necessary to reflect changes in technology, regulations, and university operations. Users will be informed of any significant changes to the policy.