International Balkan University (IBU)
Bring Your Own Device (BYOD) Policy

This BYOD (Bring Your Own Device) Policy outlines the rules and guidelines for employees, students, and visitors who wish to use personal devices (such as smartphones, tablets, laptops, etc.) to access the university's network, systems, and data. The policy's purpose is to ensure that the university's data and infrastructure are secure while providing flexibility and convenience for users.

This policy applies to all faculty, staff, students, contractors, vendors, and visitors who use personally owned devices to access the university's network, applications, or data. It covers all types of personal devices, including, but not limited to, smartphones, tablets, laptops, and wearable devices.

1. **Eligibility**
    - **Employees and Faculty**: Full-time and part-time employees, including faculty members, can use personal devices for work-related activities.
    - **Students**: Students can use personal devices to access educational resources, course materials, and university applications.
    - **Contractors & Vendors**: Third-party contractors and vendors may use personal devices only if authorized by the IT department.
    - **Visitors**: Visitors can use personal devices to access the guest Wi-Fi network, which is segregated from the main network and does not allow access to internal systems or sensitive data.
2. **Permitted Usage**
    - **Work-related Tasks**: Employees and faculty may use personal devices for work-related tasks, such as checking email, accessing calendars, conducting research, and participating in virtual meetings.
    - **Educational Purposes**: Students may use personal devices to access course materials, submit assignments, participate in online discussions, and take exams.
3. **Security Requirements**
    - **Password Protection**: All personal devices must be password-protected or use biometric security (e.g., fingerprint, facial recognition) to prevent unauthorized access.
    - **Encryption**: Devices that access university data must support encryption for both data at rest and in transit. This includes enabling disk encryption on laptops and ensuring secure, encrypted connections (e.g., VPN, SSL) for accessing university resources.
    - **Antivirus & Anti-malware**: Personal devices must have up-to-date antivirus and anti-malware software installed. Users are responsible for ensuring regular updates and scans are performed.

- **Software Updates**: Users must keep their devices' operating systems and applications updated with the latest security patches and updates.
- **Remote Wipe Capability**: The university reserves the right to require the installation of software that enables remote wiping of university data in case of a lost, stolen, or compromised device.

4. **Network Access**
    - **Segregated Networks**: Personal devices will connect to a segregated network (e.g., Student Wi-Fi) that limits access to sensitive university systems. Critical systems and data will remain on a separate network.
    - **VPN Access**: To access secure internal resources, users may be required to use a Virtual Private Network (VPN) connection. VPN usage will be monitored to ensure security compliance.
    - **Guest Network**: A separate guest network will be available for visitors and users with limited access needs. This network will not allow access to internal resources or sensitive data.
5. **Data Protection**
    - **Sensitive Data Acce**ss: Access to sensitive data (e.g., student records, employee records, research data) from personal devices is restricted and may require additional authentication measures.
    - **Data Storage**: Users must not store sensitive university data locally on personal devices. Instead, they should use secure cloud storage solutions provided by the university (e.g., OneDrive).
    - **Data Sharing:** Sharing university data via unauthorized apps (e.g., personal email accounts, social media, or cloud storage services not sanctioned by the university) is strictly prohibited.
6. **Privacy Considerations**
    - **Personal Data**: The university will not access or monitor personal data stored on personal devices. Monitoring will only apply to activities related to university systems and data.
7. **User Responsibilities**
    - **Compliance with Policies**: Users must comply with this BYOD policy and other relevant university policies, including the Acceptable Use Policy, Data Protection Policy, and Information Security Policy.
    - **Device Maintenance**: Users are responsible for maintaining their devices, including updates, repairs, and ensuring proper security measures are in place.
    - **Reporting Security Incidents**: Users must report any security incidents, including lost or stolen devices, unauthorized access, or malware infections, to the IT department immediately.
8. **IT Department Responsibilities**
    - **Support Limitations**: The IT department will provide support for configuring devices to access university resources but will only offer partial technical support for personal devices (e.g., hardware repairs).

- **Monitoring & Auditing**: The IT department will monitor network traffic from personal devices to ensure compliance with security policies. Audits may be conducted periodically.
- **Revocation of Access**: The IT department reserves the right to revoke access to the university's network or systems if a user's device is found to be non-compliant with this policy or poses a security risk.

9. Enforcement & Disciplinary Action

- **Policy Violations**: Any violations of this policy may result in disciplinary actions, including but not limited to loss of network access, confiscation of the device, or other actions deemed appropriate by the university.
- **Legal Consequences**: Unauthorized access, data breaches, or misuse of university data may result in legal action under applicable laws and regulations.

10. Policy Review and Updates

- This BYOD policy will be reviewed annually and updated as necessary to reflect changes in technology, security risks, or university requirements. Users will be notified of any significant updates or changes.