Document Title: ICT Knowledgebase – IT Security
Version: 1.0
Last Updated: 2025-04-10
Prepared by: Information and Communications Technology (ICT), AKU

ICT Knowledgebase – Topic 4: IT Security

This section explains AKU's IT Security policies, best practices, and procedures to protect information assets and ensure a secure computing environment. It covers topics such as threat reporting, multi-factor authentication, data protection, and guidelines to safeguard user credentials and devices.

Frequently Asked Questions (FAQs)

Q1: What is IT Security at AKU?
A: IT Security at AKU encompasses policies, procedures, and technologies designed to protect the confidentiality, integrity, and availability of the institution's information assets and systems.

Q2: Why is IT Security important for me as an AKU user?
A: Adhering to IT Security guidelines helps prevent unauthorized access, data breaches, and ensures the safe operation of all IT systems, thereby protecting both personal and institutional data.

Q3: What are the common IT security threats I should be aware of?
A: Common threats include phishing, malware, ransomware, social engineering, unauthorized access, and weak password practices.

Q4: How do I report a security incident or suspicious activity?
A: Immediately report any suspicious activity, phishing attempts, or security incidents to the ICT Service Desk by email (it.servicedesk@aku.edu) or phone (3434).

Q5: What is multi-factor authentication (MFA) and why should I use it?
A: MFA adds an extra layer of security by requiring a second form of verification (such as a code sent to your mobile device) in addition to your password, thereby reducing the risk of unauthorized access.

Q6: How do I enrol in multi-factor authentication (MFA)?
A: Contact the ICT Service Desk or refer to the MFA enrolment guide on the IT portal to set up MFA on your AKU account.

Q6: How do I reset multi-factor authentication (MFA) if my device is stolen?

A: The users are required to contact ICT Service Desk in case of device stolen. The ICT Service Desk will request the relevant ICT team for resetting the MFA.

Q7: How do I reset multi-factor authentication (MFA) if my device is upgraded to a new one?

A: The users are required to visit the link https://login.microsoftonline.com/ to add/modify the sign in method (Microsoft Authenticator, phone number).

Q7: What are the guidelines for creating a secure password?

A: Create passwords that are at least 8 characters long, include a mix of uppercase and lowercase letters, numbers, and special characters, and avoid using easily guessable information such as your name, date of birth etc.

Q8: How often should I change my domain password?

A: Your domain password expires every 90 days. It is recommended to change your password proactively before the expiry date to avoid lockouts.

Q9: What should I do if I receive a suspicious email or phishing attempt?

A: Do not click any links or download attachments. Forward the email to it.servicedesk@aku.edu and report the incident immediately. If you have clicked it, change your password immediately.

Q10: Are there any specific policies for accessing AKU data remotely?

A: Yes, remote access is granted only to approved users with proper VPN and MFA configurations. Refer to the IT Policy on the IT portal for details.

Q11: How can I secure my personal device when accessing AKU resources?

A: Ensure that your device has updated antivirus software, the latest security patches, and is configured according to AKU's device security guidelines.

Q12: What is the acceptable use policy for IT systems at AKU?

A: The Acceptable Use Policy defines the proper use of AKU IT resources, prohibiting activities that may compromise system security. Refer to the IT policies on the AKU portal for full details.

Q13: What measures are in place to protect sensitive data at AKU?
A: Data protection measures include encryption, access controls, regular security audits, and user education on data handling practices.

Q14: How is my data backed up and secured?
A: AKU uses robust backup systems, including cloud storage (OneDrive) and offsite data centres, to ensure that critical data is securely backed up and available for recovery in case of an incident.

Q15: What do I do if my device is lost or stolen?
A: Report the incident immediately to both the ICT Service Desk and the appropriate security department so that remote wiping or additional protective measures can be taken.

Q16: How often are IT security trainings conducted?
A: Regular IT security training sessions are organized for AKU users. Check the IT portal or internal communications for upcoming training events.

Q17: Can I use public Wi-Fi networks to access AKU systems?
A: It is not recommended to access AKU systems using public Wi-Fi. If necessary, use a secure VPN connection to protect your data.

Q18: What are the consequences of not following IT security guidelines?
A: Failure to adhere to IT security policies can result in compromised data, disciplinary actions, and potential security breaches that affect the entire institution.

Q19: How are software and system vulnerabilities managed at AKU?
A: AKU continuously monitors, updates, and patches software and systems to protect against vulnerabilities.

Q20: Where can I find more detailed IT security policies and guidelines?
A: Detailed IT security policies are available on the AKU IT portal. Users are encouraged to review these documents regularly to stay informed about best practices and requirements.

Q: Is it safe to store confidential files in OneDrive?
A: Yes, OneDrive uses enterprise-grade encryption. However, avoid sharing sensitive data without proper permissions.

Q: How do I report a phishing email?
A: Forward the suspicious email to **it.servicedesk@aku.edu** and do not click on any links.

Q: What is ransomware and how can I prevent it?
A: Ransomware is malicious software that encrypts your files. Avoid suspicious downloads, update your system, and never open unknown attachments.

Q: How often are backups performed?
A: Cloud systems like OneDrive and SharePoint sync automatically. On-premises servers are backed up regularly.

Q: Can I request data recovery from an old device?
A: No, once the old device is write-off, data cannot be retrieved. This is user responsibility to ensure that the confidential data is backed up.

Q: Can I use personal USB drives on AKU computers?
A: USB usage is restricted and monitored. Avoid using unverified external storage without ICT approval.

Q: What is AKU's internet usage policy?
A: Internet should be used for work-related purposes only. Non-work activities may be flagged during audits.

Q: Is access to personal email allowed from office systems?
A: Accessing personal email is discouraged due to security risks. Use AKU-approved platforms for communication.

Q: What happens if I breach IT policy?
A: Breaches are reviewed by ICT and HR. Disciplinary actions vary depending on severity and intent.

Q: Who should I contact about IT compliance concerns?
A: Email **it.security@aku.edu** or reach out via the Service Desk for data protection or compliance concerns.