Document Title:	Secure Onboarding Policy		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		**Document Reference/Policy No.:**	ADM-PP-004
Chief Information Officer		**Issuance Date:**	1 September 2019
		Revision Date:	24 May 2024
		Revision No.:	3.0
		Number of Pages:	16

1.0 Policy Statement: AKU implements robust security controls on all applications, databases, servers, operating systems, and network assets intended for integration into our production environment.

2.0 Terms and Definitions:

2.1. ISO: International Organization for Standardization

2.2. AKU: Aga Khan University

2.3. ICT: Information Communications Technology

3.0 Purpose: The purpose of this document is to implement security controls on all applications, databases, servers, operating systems, and network assets which will become the part of the AKU production environment and ensure that planned ICT systems comply with AKU Global Information Security policies.

4.0 Scope: This document is applicable to all applications, databases, servers, operating systems, and network assets that will become part of the AKU production environment. The scope of this document is applicable to all AKU locations globally. In case of any specific local country regulations not addressed by this policy, the local AKU entity will develop and maintain a local policy to comply with local regulatory requirements, subject to the approval of the Senior Manager, Information Security and Chief Information Officer.

5.0 Responsibility: It is the responsibility of ICT, Information Security, and relevant departments.

6.0 Process/Procedure:

6.1. Secure Onboarding of Software Applications: The application includes desktop / web / mobile and cloud-based applications. ICT Information Security review and testing scope of work includes assessment of application security weaknesses and vulnerabilities including backend databases and underlying infrastructure which can be exploited by internal or external attackers.

6.1.1. In-House Software Applications:

i. Relevant application owner / software development team will engage ICT Information security team at project initiation / requirement analysis phase to obtain software security requirements. Early involvement of the Information Security team will enable the software development team and application owner to understand and embed security requirements at the start of the project.

ii. Information Security team will share software security requirements with application owner / software development team. The requirements will include, but not be limited to, software authentication, authorization, encryption, secure coding, system logging / auditing and availability controls.

iii. During the software design and development phase, the Information Security team will review the technical design of the software application. This will include, but not be limited to, functional & technical specifications, data flow diagrams, system integration documents and network design.

iv. During the software testing phase, the Information Security team will perform software security review and testing to validate security controls as per the given security requirements. The following steps will be performed by the Information Security team:

- Perform security risk assessment as per Application Security Assessment Checklist (Refer Section: 11.0 Annexure).
- Perform secure code reviews (if necessary).
- Perform vulnerability assessment/ penetration testing (if necessary).
- Issue software application security assessment report to relevant team.
- Revalidate the reported vulnerabilities in the production environment.
- In the case of critical applications, Information Security will recommend engaging a third party/independent vendor to perform penetration testing exercises to validate the security posture of applications and underlying infrastructure.

v. In case of changes or modifications to software applications, the relevant application owner must inform the Information Security team and the application will be reassessed.

6.1.2. Off-the-shelf Applications and Software:

i. The initiator fills out information security questions in addition to software related questions in “ICT New Request Form” and sends it to Solutions and Innovations Team.

ii. The Solutions and Innovations team will review “ICT New Request Form” and engage Information Security team depending on the classification of information stored or processed by the application.

iii. Information Security team will share the security requirements/questionnaire with applications team / application owner coordinating with vendor.

iv. The Information Security team will review vendor responses received on the security requirements/questionnaire.

v. The Information Security team will review relevant documentations and specifications related to security provided by the vendor.

vi. During the application deployment phase, the Information Security team will validate security controls as per security requirements and vendor responses received at the initial phase.

vii. Finally, Information Security sends application security feedback or report to the initiator based on the security review performed.

6.2. Timeline to Complete Security Assessments:

6.2.1. Internal Security Assessment: The Information Security team will respond to requests within ten (10) working days based on in-line security projects. Internal security assessments should take no more than three (3) weeks for security fieldwork and reporting. Conformance to the timelines would be based on the timely availability of requested information from relevant application team / business owner / vendor.

6.2.2. Internal Security Assessment with External Penetration Testing: The Information Security team will respond to requests within ten (10) working days based on in-line security projects. Internal security assessment should take no more than three (3) weeks. Penetration Testing from External Vendor will require RFP/Procurement process and should take no more than three (3) weeks, while complying to Purchasing & Supply Chain Management Division (PSCMD) processes. External vendors would take approximately three (3) weeks for project execution and reporting.

6.3. Secure Onboarding of Server/Asset: Every physical / virtual server and operating system must go through the Server Assessment Checklist before being onboarded onto the AKU production environment. The checklist will be signed by the ICT infrastructure manager and a copy of the signed checklist will be shared with Information Security for record purposes.

6.4. Secure Onboarding of Network Devices: All network devices must go through the Network Assessment Checklist before being onboarded onto the AKU production environment. The checklist will be signed by the ICT infrastructure manager (network) and a copy of the signed checklist will be shared with Information Security for record purposes.

6.5. Secure Onboarding of Medical Devices: Completion of the Medical Devices Security Checklist is required for the procurement and onboarding of medical devices. The checklist will be verified before any medical devices are onboarded onto the AKU production environment.

7.0 Compliance Reference:

7.1. ISO/IEC 27001:2013 standard, Clause A.7.2 - Information Security Policy.

7.2. ISO/IEC 27001:2013 standard, clause A.12.6 - Technical vulnerability management.

8.0 Measures of Compliance: Compliance with this policy will be verified through internal and external audits.

9.0 Reference: This document satisfies the following requirements of the ISO27001:2013

Clause Reference	Name of the Clause	Control reference	Name of control	Name of the Standard
-	-	A.12	Operations Security	ISO/IEC 27001:2013
-	-	A.12.6	Technical Vulnerability Management	ISO/IEC 27001:2013

10.0 Related Institutional Documents: Information Security Policy Manual (ADM-P-024).

11.0 Annexures:

Application Security Assessment Checklist			
Application Information			
1	Name of the Application		
2	Application Owner		
3	Brief Description of Application		
4	Where will the application be hosted? Ie., at AKU data center or outsourced to an external 3rd party (Cloud)?		
5	Application will be developed by In-house software development team or outside software vendor?		
6	Is this an internet facing application?		
7	What is the confidentiality and inherent risk of application data?		
S#	**Application Security Controls / Questions**	**List of Requirements**	**Comments/Issues**
1	Has an independent vulnerability assessment, penetration testing, and source code review been performed for the Software Application?		
2	Has vulnerability assessment been conducted for underlying OS and DB components for this application?		
3	Has the application owner defined application roles and privileges that would be allocated to users ensuring confidentiality and segregation of duties?		
4	Does the application provide Role-Based Access Control (RBAC) functionality to ensure system access on a need-to-know basis and enables security administrator to assign permissions and restrictions in a complex, matrixed set of authorizations for individual users to access the application record?		
5	Does the software provide the functionality to generate reports for User Access Rights with the following information: • User Name • User Creation Date • User Access level • User Roles / Menus / Privileges • User Revocation / Disabled Date • User Modification Date (roles/profiles/menus/privileges changed or granted) • User Last Login Date • User Status (active or disabled)		
6	Does the application use a unique login id for each user?		

7	Does the application prompt newly created users to change the initial password? (Password change at first log-on)		
8	Are the password settings configured in accordance to AKU's Information Security Policy: ▪ Minimum password length should be configured as eight (8) characters. ▪ Application should only accept alphanumeric passwords. ▪ Application users should be forced to change their passwords after 90 days.		
9	Are the account lockout settings configured in accordance to AKU's Information Security Policy? User accounts should be locked after 5 consecutive failed logon attempts.		
10	Does the application have the ability to generate audit reports for specific or all users' application activity? Is software logging enabled with at least the following user events: ▪ Failed login attempts ▪ Logon access on software configuration and setup functions.		
11	Does the application have time-stamp functionality (user, role, date, & time) with respect to records processed in the application? Can a user audit trail be generated for system processed records?		
	Does the application allow an authorized administrator to enable or disable auditing for events or groups of related events?		
12	Is an idle session time out centrally configured in the application?		
13	Are appropriate access allocation, modification and revocation procedures documented for the application?		
14	Are all unnecessary services, default accounts disabled / removed or protected to prevent their unauthorized use on the application and its underlying OS and DB?		
15	Has the application owner identified the data backup and disaster recovery needs of the application?		
16	Is the application software, database and O/S supported by vendor/ OEM?		
17	Is the application included in the application assets inventory of AKU?		
18	Does the application prevent a security / user administrator from performing business transactions that conflict with his/her role?		
19	Application password fields do not display the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.		

20	The forgotten password function and other recovery paths do not reveal the current password and the new password is not sent in clear text to the user.		
21	The username enumeration is not possible via login, password reset, or forgot account functionality.		
22	Is the authentication mechanism implemented for end users?		
23	Is the authentication mechanism implemented for administrator?		
24	Does the application use a generic message for login attempts failures and account lockout?		
25	Does the application allow users to completely logout from the application?		
26	All pages that require authentication to access them have logout links.		
27	The session id is never disclosed other than in cookie headers; particularly in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.		
28	The session id is changed on each login.		
29	The session id is changed on re-authentication.		
30	The session id is changed or cleared on logout.		
31	Verify that the application does not permit duplicate concurrent user sessions, originating from different machines.		
32	Does the application encrypt session cookies?		
33	Is there a centralized mechanism (including libraries that call external authorization services) for protecting access to each type of protected resource?		
34	Single/Centralized input validation control is used by the application for each type of data that is accepted.		
35	Password hashes are salted uniquely when they are created.		
36	All code implementing or using error handling and logging controls are not affected by any malicious code.		
37	List which types of Data Encryption Mechanisms are currently incorporated at Applications Server, Database and Client Level to ensure protection against unauthorized access to applications data transmitted over an electronic communication network.		
38	Does the application encrypt sensitive data such as PII (Personally Identifiable Information), authentication data and business sensitive information during data transmission and storage?		

39	All forms containing sensitive information have disabled client-side caching, including autocomplete features.		
40	Does the application limit the length of each user input field?		
41	If the application supports file upload functionality, does it enforce the following: a. Validate file extension/type, and file format. b. Run virus/malware scan on the uploaded file.		
42	Can the application integrate with SIEM?		
43	SSL/TLS connection failures are logged.		
Additional Security Controls for Mobile Applications			
1	Does the application encrypt sensitive data such as PII (Personal Identifiable Information), authentication data and business sensitive information during data transmission and storage?		
2	Does the application provide Role-Based Access Control (RBAC) functionality to ensure system access on a need-to-know basis?		
3	Does the application enforce an expiration of session ID's after logout?		
4	Does the application provide a functionality to terminate all linked multiple backend/host sessions after the user session is terminated?		
5	Does the application provide an audit trail of security events/violations including access information (Device ID, device address, etc.) and anomalous events?		
6	Does the application have controls to prevent logging of sensitive information such as PINs and passwords especially in transaction and interface logs?		
7	Does the application prompt to change the initial password of newly created users? (Password change at first log-on)?		
8	Are the password settings configured in accordance to AKU's Information Security Policy: ▪ Minimum password length should be configured as eight (8) characters. ▪ Application should only accept alphanumeric passwords. ▪ Application users should be forced to change their passwords after 90 days.		
9	Are the account lockout settings configured in accordance to AKU's Information Security		

	Policy? User accounts should be locked after 5 consecutive failed logon attempts.		
10	Does the application provide security configuration to protect application data such as log files and cookies to protect against alteration or compromise during data synchronization with phone device?		
11	Does application have code obfuscation in place such that source code is not easily reversible?		
12	Does application have root detection implemented to validate if mobile device is rooted or not?		
13	Application should not store sensitive data, credentials and system information in the log files to prevent side channel data leakage.		
14	Application should have configured SSL certificate pinned to the mobile application.		
15	Application should protect screenshots of sensitive screens and should not allow screenshots taken by other apps, to ensure secure displays.		
16	Application should encrypt/encode critical information in source code. Application should not save critical information in source code.		
Additional Security Controls for Cloud Applications			
1	Does the service provider use public cloud services like Azure and AWS for application hosting (SaaS) OR do they have their own cloud services and Datacenter?		
2	How is confidentiality and integrity of customer's (AKU Data) managed by the cloud service provider?		
3	How will the service provider ensure separate tenancy of AKU systems?		
4	How will the service provider ensure our applications data is segregated from other organization's data which is hosted in the service provider's cloud platform?		
5	How is the administrative access to customer's data managed, monitored, and audited by the cloud service vendor within its data center?		
6	Have the cloud service platform security controls been tested by a third party? (Provide the response with evidence)		
7	Are the information security policies and procedures of the cloud service provider aligned with the security standard ISO/IEC 27001:2013? Is the cloud vendor's information security management system ISO:27001 certified? (Provide response with evidence)		
8	How do service providers maintain the security of their datacenter? Provide the list of security controls implemented in datacenter.		

9	Has independent vulnerability assessment and penetration testing been performed for the Cloud Platform? (Provide response with evidence)		
10	What would be the mechanism to backup our applications and databases hosted at the Datacenter?		
11	What is the expected availability of the cloud platform? How will the service provider ensure 99.9% system availability?		
12	How will the service provider maintain disaster recovery and high availability of our systems?		
13	How does the cloud platform ensure data encryption at rest and in transit?		
14	How is the entire system protected from Internet threats?		
15	If we need to scale-up our application's environment, what would be the mechanism?		
16	Does the service provider require VPN connectivity between AKU and their datacenter? Do they require permanent VPN connectivity or temporary?		

Server Assessment Checklist		
Server Information		
Server Name		
Server Description		
Domain	**Controls**	**Response**
Pre-Installation Phase		
Preparation and Installation	If machine is a new installation, protect it from hostile network traffic, until the operating system is hardened.	
Post-Installation Phase for Windows Server only		
Preparation and Installation	Operating System License has been activated?	
Service Packs, Patches, Hot fixes	Are Operating system patches installed?	
	Move domain joined server to appropriate OU in order to apply policies.	
	Individual (non-generic) user accounts are created for authorized persons only with limited access rights.	
	Unused user accounts are deleted or disabled e.g. guest?	
	Is access to the server / services restricted to authorized individuals or network segments?	
	Have default administrator accounts like root, admin, sa, system been renamed (where technically possible),	

Access Control & Accounting	and their passwords split and escrowed under DUAL custody?	
	Server should be accessible from jump server.	
	Device / server is configured to perform server patching and reporting Server Patching and reporting required SCCM agent.	
	If SNMP is enabled then have Community Strings changed?	
	Server is configured for monitoring by SCOM	
	Device / server is configured to sends its performance status to SCOM?	
System Time Settings	Server is configured to synchronize its time from Secure central NTP Server	
	Server date/time and its time zone are correctly configured?	
Server Protection	Antivirus software is installed?	
	Is antivirus software configured to receive its update from the server?	
	Is the latest version of antispyware / antimalware software installed? And configured to receive its update form the server?	
Vulnerability Assessment (IT Security Role)	Is the VA of the Server performed?	

Pre-Installation Phase only for Linux / Ubuntu	
Controls	**Response**
Change root password	
Monitor server availability status	
Server access from jump server	
Is access to the server / services restricted to authorized individuals or network segments?	
Approvals	
Manager (IT Infrastructure)	
Name	
Designation	
Signature / Date	
Comments	

Network Devices Security Checklist				
Device Information				
Network Device Name				
Description / Model				
S.No	**Feature**	**Controls**	**List of Requirements**	**Comments/Notes**
1	**Restrict Infrastructure Device Accessibility**	Disable all terminal and management ports that are not explicitly required or actively being used		
		Only permit device access through required and supported services and protocols, using only secure access protocols such as SSH and HTTPS where possible		

		Only accept access attempts to authorized ports and services from authorized originators		
		Deny unused and unnecessary terminal and management services and protocols, e.g. telnet, HTTP		
		Authenticate all terminal and management access using centralized (or local) AAA		
		Authenticate all EXEC level terminal and management access using centralized (or local) AAA		
		Authorize all interactive and privileged EXEC level device management access using centralized (or local) AAA		
2	**Enforce Session Management**	Enforce an idle timeout to detect and close inactive sessions		
		Enforce an active session timeout to restrict the maximum duration of a session prior to re-authentication		
		Detect and close hung sessions, e.g. using keep lives		
3	**Restrict Device Access Vulnerability to Dictionary and DOS Attacks**	Enforce a strong password policy (may be done on the AAA server)		
		Restrict the frequency of login attempts		
		Enforce a lockout period upon multiple authentication failure attempts within a defined time window (may be done on the AAA server)		
		Restrict the maximum number of concurrent sessions		
4	**Legal Notification**	Present legal notification banner upon all terminal, management and privileged EXEC level access		
5	**AAA Server Communication Security**	Employ strong secrets for authentication between the AAA server and NAS		
		Restrict AAA communication to only the limited set of authorized AAA servers, and over the configured AAA communication ports		
6	**Web-based GUI Access**	Disable HTTP/HTTPS access if not required		
		Restrict access to HTTPS only if web access required		

		Authenticate and authorize all web access using centralized (or local) AAA		
		Enforce an idle timeout to detect and close inactive sessions		
		Enforce an active session timeout to restrict the maximum duration of a session prior to re-authentication		
		Detect and close hung sessions, e.g. using keep lives		
		Restrict the permitted rate of login attempts		
		Restrict the maximum number of concurrent sessions		
7	**SNMP Access**	Only use SNMP v3 where possible		
		Delete default community strings		
		Only permit SNMP access from authorized originators		
		Only enable minimum required access, e.g. read-only Define strong, non-trivial community strings where SNMP required		
8	**Locally Stored Information Protection (Backups)**	Enforce strong encryption of locally stored information for backups.		
9	**Infrastructure Device Management Access Logging**	Configure NTP across all devices (see NTP section for details)		
		Log all successful interactive device management access using centralized AAA or an alternative, e.g. AAA logs		
		Log all successful privileged EXEC level device management access using centralized AAA or an alternative, e.g. AAA logs		
		Log all failed interactive device management access using centralized AAA or an alternative, e.g. AAA logs		
		Log all failed privileged EXEC level device management access using centralized AAA or an alternative, e.g. AAA logs		
		Log all commands entered at a privileged EXEC level using centralized AAA or an alternative		

		Device software image verification, e.g. MD5		
11	**Device Management Best Common Practices**	Assign unique, per-user accounts (AAA)		
		Change default passwords		
		Force users to periodically change their password		
		Use TACACS+ for administrative device access where possible		
		Define multiple NTP servers for redundancy		
Additional Checks for Internet Firewall				
12	**Rule sets Order**	(implicit deny and whitelisting)		
		Deny and log (log traffic for analysis)		
13	**Application Based Firewall**	The administrators monitor any attempts to violate the security policy using the audit logs generated by the application level firewall.		
		There is a process/automated function to update the application level firewall's vulnerabilities checked to the most current vulnerabilities		
		There is a process/automated function to update the signatures with the latest attacks		
		Only authorized users are being authenticated by the application level firewall.		
14	**Stateful Inspection**	Appropriate rules are set up in terms of source and destination IP's, source and destination ports and timeouts.		
15	**Logging**	Logging is enabled and the logs are reviewed to identify any potential patterns that could indicate an attack.		
16	**Patches and Updates**	Latest patches and updates relating to firewall product are installed where applicable.		
		Signatures and other necessary updates downloaded from the vendors' trusted site.		

Approvals	
Manager IT Infrastructure (Network)	
Name	
Designation	
Signature / Date	

Comments	

Medical Devices Security Checklist			
Device Information			
Medical Device Name			
Description / Model			
S#	**Controls Checklist**	**List of Requirements**	**Comments/Issues**
1	Specify the operating system and its version comes as default with the Medical Device.		
2	Does Medical Device operating system accept latest updates, anti-virus /malware and security patch updates as soon as they become available? Does Medical Device operate as normal after patching or operating system upgrade?		
3	Is this an IoT Medical Device and connects / transmits data to the internet and website? If yes, then specify what information is transmitted to the internet and how software maintains information security and integrity? Provide latest report of Independent Penetration Testing of the Medical Device Web Interface.		
4	Has an independent vulnerability assessment and penetration testing been performed for the medical device and its software? Does the vendor have ongoing internal process of Vulnerability Assessment and Penetration Testing of the Medical Device Software? (Provide a brief description of the process).		
5	Does the vendor have a process to provide Security Updates and Patches of Medical Device Software to their customers? What is the frequency of Security Updates and Patches?		
6	If this a Wi-Fi enabled Medical Device? Does it support WPA2 (Wireless Protected Access) standard?		
7	Can communication ports which are not required for the intended use of the Medical Device be disabled?		
8	Does the Medical Device encrypt data at rest and at transmission via network? (List which type of Data Encryption Mechanism is currently incorporated in the Medical Device).		
9	Is there documentation available on what medical information is communicated with the medical device, how it is transferred and how the data is secured?		

10	Does the Medical Device support unique user/operator-specific IDs and password(s) for multiple users?		
11	Does the Medical Device use managed AD services for identification and authentication?		
12	Does the Medical Device allow one to configure and update following AKU specific Password Security Policies: ▪ Minimum password length should be configured as eight (8) characters. ▪ Application should only accept alphanumeric passwords. ▪ Application users should be forced to change their passwords after 90 days. ▪ User accounts should be locked after 5 consecutive failed logon attempts		
13	Does the Medical Device create an audit trail? If so, can it list the events that are logged, such as logons, transactions, and transmissions and filename access?		
14	Does the Medical Device auto-logoff screen lock the user after a period of inactivity?		
15	Are USB / Removable media ports enabled on the Medical device? Does the Medical Device have the functionality to disable USB / Removable media ports in the device?		

Approvals	
Manager (Bio-Medical)	
Name / Designation	
Signature	
Comments	
Manager (Infrastructure)	
Name / Designation	
Signature	
Comments	
Head of Global Information Security	
Name / Designation	
Signature	
Comments	

12.0 Author(s):

Name	Designation
Suneel Kumar Panjwani	Head of Information Security
Saad Ameen	Information Security Specialist
Atif Ali	Information Security Analyst
Samra Sabir	Information Security Analyst

13.0 Key Searchable Terms: Policy Statement, Scope, In-house, Off-the Shelf, Vulnerability Assessment and Secure On-boarding.

14.0 Revision History: This policy is subject to review and revision every two (2) years to ensure its effectiveness and alignment with changing organizational requirements and regulatory obligations.

15.0 Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change
03	24-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-