Aga Khan University Hospital

Document Title:	Incident Reporting and Response		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		**Document Reference/Policy No.:**	ADM-P-020
Chief Information Officer		**Issuance Date:**	20 November 2016
		Revision Date:	24 May 2024
		Revision No.:	3.0
		Number of Pages:	3

1.0 Policy Statement: The Aga Khan University (AKU) is committed to safeguarding its information assets, information systems, and networks. This document delineates AKU's Policy on Incident Reporting and Response to ensure the preservation of availability, confidentiality, and integrity of university information in the event of an information security incident.

2.0 Terms and Definitions: No specific terms or definitions required for this document.

3.0 Purpose: This document outlines the Aga Khan University's (AKU) Incident Reporting and Response policy. This policy exists to assure a response is conducted in a consistent manner, with appropriate leadership and technical resources, during any information security incident that may threaten the availability, confidentiality, or integrity of AKU's information assets, information systems or networks. The objective of the policy is to ensure prompt restoration of systems and operations impacted by any such incident; incidents may include access to sensitive or confidential data/ intellectual property, damage to public image, and/or damage to critical internal systems.

4.0 Scope: All users

5.0 Responsibility: All students, faculty, staff, and trainees are expected to follow this policy.

6.0 Process / Procedure / Policy Content:

6.1. Users must report any weaknesses related to ICT security and any incidents of possible security or policy breach by contacting the ICT Service Desk. The ICT Service Desk will forward such reported issues to the ICT Security team for action and response.

6.2. Depending on the nature of the incident, this may involve but not be limited to the following:

6.2.1. Collecting and analyzing evidence.

6.2.2. Determining responsible parties.

6.2.3. Assessing damages.

6.2.4. Restoring data from backup files

6.2.5. Correcting security vulnerabilities

6.2.6. Implementing appropriate security controls

6.2.7. Revising security guidelines and procedures

6.2.8. Taking disciplinary action in accordance with appropriate AKU policies

6.2.9. Reporting incidents to appropriate authorities.

6.3. In cases where a user account is compromised or hacked, the following steps will be performed immediately to prevent it from spreading malicious emails and causing harm to other email accounts and AKU network.

6.3.1. Change User Password

6.3.2. Disable Computer Login and Email Access

6.3.3. Inform ICT Service Desk (SD) of the account compromised so that they can inform user accordingly.

6.3.4. SD will send an analyst to have the user PC checked for any malware or viruses.

6.3.5. Any malware or viruses found will be cleaned.

6.3.6. The analyst will also educate the user by asking them to keep a complex password, keep changing it regularly, avoid clicking or replying to suspicious spam emails and not sharing their password with anyone.

6.3.7. Login and email access will be restored after the above conditions are fulfilled.

6.3.8. In case if user is restricted to send emails outside AKU (other than @aku.edu email addresses) and gets a ‘failure to deliver’ email (also called NDR or Non-Delivery Report), the NDR email would be requested from the user so that the user can be delisted from the block sender list of our Anti-Spam service.

6.3.9. Confirm from the user if they are able to use their account like before, once they are delisted on the Anti-spam service.

7.0 Disciplinary Actions: The failure by the users to comply with these Policies may result in loss of access to some or all of ICT Resources and/or loss of access privileges to ICT Resources. In addition, violators of these Policies may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.

8.0 Compliance Reference: No specific regulatory reference is provided for this policy.

9.0 Measures of Compliance: No specific measures of compliance.

10.0 Reference: No specific references provided.

11.0 Related Institutional Documents: No related documents applicable.

12.0 Annexures: No additional documents provided.

13.0 Author: Muhammad Fahd, Director ICT Global Service Delivery.

14.0 Key Searchable Terms: Incident Response.

15.0 Documents Change Record:

Review #	**Review Date** (dd-mm-yyyy)	**Description Of Change**	**Identification of Change**
3.0	24-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-