1. PURPOSE

1.1 The purpose of this policy is to set the security control required for timely and effective handling and management of information security incidents.

2. APPLICABILITY:

2.1 All employees; Administrative staff, Head of Departments, Directors, faculty, enrolled students, contractors, third-party, or electronic affiliate services of the Prince Sultan Military College of Health Sciences.

3. RESPONSIBILITY:

3.1 This policy applies to all employees and short/long term contractors who handle PSMCHS assets including but not limited to sensitive information or sensitive information entrusted to PSMCHS regardless of geographical location.

4. DEFINITION OF TERMS:

None.

5. POLICY:

5.1 The PSMCHS's Policy for Managing Information Security Incidents (including Data Breaches) will set out the procedures and guidelines for reporting and managing data breaches and other information security incidents

5.2 An information security and ASSETS incident is a suspected or confirmed violation of the integrity, availability, or confidentiality of the information that could cause or has caused harm to the organization. The incident can be in the form of the following

- 5.2.1 Suspected/Successful hacking attempts
- 5.2.2 Accidental loss of information
- 5.2.3 Hardware resources and components lost/stolen/ Theft of equipment
- 5.2.4 Virus incidents regarding Email, Internet, CD, diskette and others
- 5.2.5 Failure/crash of IT equipment
- 5.2.6 Power problems and loss of data
- 5.2.7 Natural disaster, such as flood, fire
- 5.2.8 Hardware, Software, and Operational errors resulting in erroneous data
- 5.2.9 Violation of Security Policies

6. PROCEDURES:

6.1 Prince Sultan Military College of Health Sciences (PSMCHS) ITCD must develop, and implement formal systems and procedures for detecting and reporting security incidents.

6.2 All security incidents must be communicated on time and through the appropriate authorities to ensure adequate corrective actions are taken immediately.

6.3 A standard "Incident Handling Form" **AS FORM CS-005 Incident Report Form** must be produced in order to report all security violations/incidents including at least the following information:

- 6.3.1 Incident Date and Time
- 6.3.2 Causes
- 6.3.3 Affected Business, Services, and Magnitude
- 6.3.4 Expected Recovery Date and Time
- 6.3.5 Next Follow-up

6.4 Based on available data and the level of criticality of an incident, ITCD or relative responsible party should review the incident report. Upon validation, ITCD must perform an incident assessment to measure its magnitude and recommend proper actions.

6.5 Preventive action must be taken by sending out incident alerts to application groups and user departments, which could possibly be affected by similar incidents.

6.6 The available effective mechanism must be utilized to measure the incident and its impact.

6.7 Based on the incident and its effect, Information Security should recommend any update in the available security policies, enhancement or implementation of new controls, where applicable to limit the frequency of occurrence.

6.8 Incident evidence and reports must be secured and preserved properly as this might be needed for further investigations.

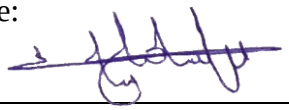
6.9 Detailed documentation specifying the history of incidents must be maintained with PSMCHS ITCD. This record will contain the information, which could be used for managing future risks and contributing to establishing the appropriate controls for the PSMCHS environment.

7. REFERENCES:

7.1 None.

8. APPENDICES:

8.1 None

Compiled by: **Engr. Turki Mohammed Al Hayyan** *Assistant of ITCD Director*	Signature: 	Date: 01/11/2021
Reviewed by: **Capt. Turki Mohammed Al Harbi** *ITCD Director*	Signature:	Date: 01/11/2021
Authorized by: **Brig. Gen. / Dr. Mohamad J. Al Zahrani** *Vice Dean of Development and Quality*	Signature:	Date:
Approved by: **Dr. Eidan Mousa Al Zahrani** *Dean of Princes Sultan Military College of Health Sciences*	Signature:	Date:
Date effective *(1st Issue)* or Date revised *(2nd Issue and onwards):01/11/2019*	Date of next review: 01/11/2021	