Information Security Policy

1.0 Purpose
The purpose of this Policy is to establish a framework of minimum standards and best practices for the security of HCT’s digital Information and/or data and lay down course of actions to protect the information assets of HCT from threats, whether internal or external, deliberate or accidental, thereby ensuring that security and services are uninterrupted.

2.0 Scope
This Policy is applicable to staff, faculty, students, external parties and to all users of HCT’s digital information assets, whether they are officially affiliated with HCT or not, and whether on campus or from remote locations.

This Policy applies to all devices, both HCT-owned computers (including those purchased with grant funds) and personally-owned or leased computers that connect to the HCT network and store HCT information. It also applies to those who collaborate with HCT to provide or receive services or information; therefore contracts and agreements shall include statements whereby the contractor/partner agrees to comply with this Policy.

3.0 Control and Distribution
1. The VP Education Technologies is the owner of this Policy. The VP Education Technologies shall ensure that this Information Security Policy is a true and accurate representation of the applicable policies and procedures and that it is kept up to date at all times.
2. All requests for revisions shall be addressed to the VP Education Technologies. Amendments shall be made, if any are required, after approval as per the DoA, and superseded versions of the policies shall be retained for future reference.
3. Date of next review: 23 April 2022

4.0 Definitions
Refer to Education Technologies Glossary for the definition of terms and abbreviations.

5.0 Roles and Responsibilities
1. Education Technologies Information Security Unit: Part of the Education Technologies division, the Information Security unit manages the overall security of HCT data and network and is responsible for the following:
   - Planning, designing and implementing access control, network security and Information Security assurance framework.
   - Developing Education Technologies related policies, processes, standards and compliance measures for the overall security framework.
   - Monitoring and measuring the internal control systems to ensure compliance with the Education Technologies security framework, and ensure appropriate access levels are maintained and updated.
   - Providing awareness of the Information Security policies/procedures to HCT employees, guests, and vendors.

2. Data Custodians - The Data Custodian is responsible for:
   - Labeling data with the appropriate classification and applying required and suggested safeguards
   - Implementing the policies and guidelines established by the Data Trustees and Owners

V 1.0 Issue Date: 23/4/2020
HCT-POL-EDT-017  Information Security Policy

This document is uncontrolled if found in printed form or retrieved from sources other than the portal. Please refer to the portal for the latest version.

https://pms.hct.ac.ae/pages/HCT-POL-EDT-017.aspx
- Physical data storage, backup and recovery, and the operation of security and data management systems etc.

3. **Data Owners**: Manager level staff that are responsible for the operation and appropriate classification of data.

4. **Data Trustees**: Senior management or the stakeholders who have planning and Policy-level responsibility for data within their functional areas and management responsibility for defined segments of institutional data.

5. **Data Consumers/Users**: Responsible for complying with data use requirements. Data Users also have a critical role to protect and maintain the confidentiality and integrity of HCT information systems and data. For the purpose of information security, a Data User is any employee, contractor, student or third-party provider who is authorized by the Data Owner to access information assets.

6.0 Policy Statements

HCT is committed towards securing the confidentiality, integrity and availability of information for the business operations. The security of information is therefore regarded as vital for the successful business operation of HCT and their employees.

1. All application information assets and legal/ regulatory requirements shall be addressed as per HCT Strategic goals and objectives.

2. All Users (including Students, Employees, Consultants) of HCT Digital Assets (including data/ information) have the responsibility of ensuring that the information/ data is used in a secured and appropriate manner.

3. All User of HCT digital assets have the responsibility of reporting any issues noted with respect information security to the appropriate authorities within the Ed Tech.

4. Detailed log should be maintained to record the IS incidents and HCT’s response to it.

5. Information Security Risk Assessment framework shall be developed and/or reviewed annually to assess and track the risks and its controls.

6. Appropriate Information Security Awareness training is mandatory to all the HCT employees, students, consultants and contract staff.

7. Employees and vendors or third party contractors shall adhere to the information security policies, procedures, standards, guidelines etc. approved by the management of HCT.

8. Information and Information Processing systems shall be handled securely to avoid any loss related to confidentiality, integrity and availability through appropriate access controls such as blocking the USB, any I/O devices (except HCT owned printers, mouse and keyboards) which is as per Ed Tech/ IS Policies, Procedures and Guidelines.

9. All the end users’ passwords shall be as per complexity defined by Information Security Policies, Procedures/ Guidelines and shall expire on 90th day.

10. Confirmed information security incidents shall be investigated, managed and worked upon on a timely manner based on the severity and escalation matrix defined as per the Managed Security Services agreement.

11. IT Business Continuity plans shall be defined, implemented and tested adequately to ensure availability of information and information processing systems during any emergency.

12. Employees and non-employees of HCT shall not attempt to circumvent or subvert any of the information security controls.

13. All HCT employees, students, consultants and contract staff to ensure compliance with applicable standards and regulations on information security e.g. ISO 27001:2013 and NESA.

14. Any violation or breach of this Policy shall be subject to HCT HR disciplinary procedure in accordance with the HR Policy.

15. If users are unsure or unclear about any aspect in this Policy, they should seek clarification or advice from the Information Security team.

16. The Information Security team reserves the right to check the compliance with this Policy on a periodic basis.
17. Any exceptions to this Policy with valid business justification require approval from VP Education Technologies and if required from the Executive Committee. All the exceptions should be formally documented and revisited periodically if still applicable/appropriate.

7.0 Related Documents
- HCT-GDL-EDT-001 Information Security Guidelines
- HCT-POL-EDT-010 Disaster Recovery Management Policy
- Education Technologies Glossary
  (/Other%20Related%20Documents/Education%20Technologies%20Glossary.pdf)

Version Control and Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Amendment details</th>
<th>Review and approval details</th>
</tr>
</thead>
</table>

V 1.0  Issue Date: 23/4/2020  HCT-POL-EDT-017  Information Security Policy

This document is uncontrolled if found in printed form or retrieved from sources other than the portal. Please refer to the portal for the latest version.

https://pms.hct.ac.ae/pages/HCT-POL-EDT-017.aspx