IT Security Policy
Version 1.0
Information Systems & Technology Department
Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Authors</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>26th October 2014</td>
<td>Abdel Ghafour Al Ali (Information Security Engineer)</td>
<td>First Draft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Saif Salem Bamadhaf (Acting Manager, Information Security)</td>
<td></td>
</tr>
</tbody>
</table>

Document Acceptance and Release Notice

This is version 1.0 of the Higher Colleges of Technology IT Security Policy. This IT Security Policy is a controlled and managed document. For identification of amendments, each page contains the version number and page number. Changes will be issued only as a complete document. Recipients should remove superseded versions from circulation. This document is authorized for release after all signatures below have been obtained.

A review and update of this document will take place on annual basis or when changes require revising the IT Security Policy. Such modifications shall relate to changes in roles and responsibilities, release of new legislation or technical guidance or the identification of a new policy area. The HCT Executive Committee, in consultation with appropriate parties, will approve all revisions to this IT Security Policy. When approved, a new version of the IT Security Policy will be issued, and all affected parties/personnel will be informed of the changes.

Any requests for changes should be submitted to the owner or author of this document.

Approvals

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr. Saif Salem Bamadhaf</td>
<td>Chief Technology Officer</td>
<td>19/4/2015</td>
<td></td>
</tr>
<tr>
<td>Ms. Khulood Al Mualla</td>
<td>Deputy Vice Chancellor – Administration</td>
<td>23/4/2015</td>
<td></td>
</tr>
<tr>
<td>Dr. Abdullatif Al Shamsi</td>
<td>Vice Chancellor</td>
<td>4/5/2015</td>
<td></td>
</tr>
<tr>
<td>H.E. Omran Al Shamsi</td>
<td>Chancellor</td>
<td>10.5.2015</td>
<td></td>
</tr>
<tr>
<td>Document Number</td>
<td>CSIT/IT Security Policy/v1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document Name</td>
<td>Higher Colleges of Technology IT Security Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date Created (Draft)</td>
<td>26th October 2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date Approved</td>
<td>Refer to Document Acceptance and Release Notice (Page 5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Central Service IT, Block F, Central Services, Abu Dhabi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium of Distribution</td>
<td>Electronic PDF and Word Document</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Classification</td>
<td>Internal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retention</td>
<td>5 years</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Archive Location</td>
<td>Central Services IT Web site</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(<a href="https://portal.hct.ac.ae/sites/ITS">https://portal.hct.ac.ae/sites/ITS</a>)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- This document should be distributed to:

<table>
<thead>
<tr>
<th>Title</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the College Directors</td>
<td>Electronic Copy, Booklet</td>
</tr>
<tr>
<td>All the Policy Council Members</td>
<td>Electronic Copy, Booklet</td>
</tr>
</tbody>
</table>

- This document should be published:

<table>
<thead>
<tr>
<th>Location</th>
<th>Format</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCT Portal</td>
<td>Electronic Copy</td>
<td>Information Systems and Technology Department</td>
</tr>
</tbody>
</table>

- This document affects the following parties:

**Affected Parties**

All the HCT users including but not limited to staff, students, contractors, third party individual directly or indirectly involved with HCT's business activities.
Contents

Introduction: ......................................................................................................................................................... 3
Policy Handbook Scope: ........................................................................................................................................ 5
HCT’s IT Security Mission Statement: ..................................................................................................................... 5
Objectives: ............................................................................................................................................................. 5
Responsibilities and Undertaking: ........................................................................................................................ 6
Compliance: ........................................................................................................................................................... 6
Audit and Review: .................................................................................................................................................. 6
1.0 Anti-Virus Policy - GP 450 ............................................................................................................................. 7
2.0 Password Management Policy - GP 451 ....................................................................................................... 9
3.0 Internet Usage Policy - GP 452 ................................................................................................................... 12
4.0 E-mail Usage Policy - GP 453 ...................................................................................................................... 14
5.0 Information Classification Policy - GP 454 .................................................................................................. 16
6.0 Bring Your Own Device Policy (BYOD) - GP 455 .................................................................................... 19
7.0 Desktop & Laptop Usage Policy - GP 456 ................................................................................................... 20
8.0 Software Compliance Policy - GP 457 ........................................................................................................... 22
9.0 Back-up and Restoration Policy - GP 458 .................................................................................................. 24
10.0 Remote Access Policy - GP 459 ................................................................................................................ 28
11.0 Wireless Communication Policy - GP 460 ................................................................................................. 30
12.0 Mobile Phone Policy - GP 461 .................................................................................................................... 31
13.0 Dispose of Media Policy - GP 462 ............................................................................................................. 32
14.0 Physical Access for Data Center Policy - GP 463 .................................................................................... 33
15.0 Patch Management Policy - GP 464 ......................................................................................................... 34
16.0 Change Management Policy - GP 465 ...................................................................................................... 36
17.0 User Access Management Policy - GP 466 ............................................................................................. 38
18.0 Information Security and Business Continuity Incident Management Policy - GP 467 .................... 40
19.0 Acceptable Use of IT Equipment Policy - GP 468 .................................................................................. 43
20.0 Clear Desk and Clear Screen Policy - GP 469 ......................................................................................... 45
21.0 Log Management Policy - GP 470 ........................................................................................................... 46
22.0 Data Storage Policy - GP 471 .................................................................................................................... 49
23.0 Database Management Policy - GP 472 ................................................................................................. 50
Roles and Responsibilities: .................................................................................................................................. 51
IT Security Policy Task Force ................................................................. 52
Glossary: .................................................................................................. 53
Introduction:

The IT Security Policy is defined as a set of standards, guidelines and procedures that specify the expectations in regard to the appropriate use of information, information assets and network infrastructure. IT Security Policy is approved and supported by the senior management of HCT. The intentions for publishing an IT Security Policy is not to impose restrictions that are contrary to the Higher Colleges of Technology’s (HCT) established culture of openness, trust and integrity; however, it is the Information Technology Department’s commitment to protect the HCT and its students and staff from illegal or damaging actions by individuals, either intentionally or unintentionally.

HCT Information Technology (IT) infrastructure, including but not limited to computer equipment, software, operating systems, applications, data storage media, user accounts providing electronic mail, Internet browsing, and FTP, are the property of the organization. These systems are to be used for academic and administrative purposes in serving the interests of the HCT, and of our students and staff in the course of their normal business operations.

Adapting these policies will assist in complying with Information Security Management standard (ISO 27001:2013) and Business Continuity (BS 25999-2:2007).

Effective security is a department effort involving the participation and support of every student and staff in the HCT and affiliate who deals with information or information systems. It is the responsibility of every user using the HCT’s resources to know these standards, guidelines and procedures and conduct their activities in compliance to this policy.

IT Security policy is governed by the approved Delegation of Authority (DoA) Matrix. The IT Security Policy contains and is not limited to the following sub-policies to be adhered by all student, staff and authorized third party personnel:

1.0 Anti-Virus Policy - GP 450
2.0 Password Management Policy - GP 451
3.0 Internet Usage Policy - GP 452
4.0 E-mail Usage Policy - GP 453
5.0 Information Classification Policy - GP 454
6.0 Bring Your Own Device Policy (BYOD) - GP 455
7.0 Desktop & Laptop Usage Policy - GP 456
8.0 Software Compliance Policy - GP 457
9.0 Backup and Restoration Policy - GP 458
10.0 Remote Access Policy - GP 459
11.0 Wireless Communication Policy - GP 460
12.0 Mobile Phone Policy - GP 461
13.0 Dispose of Media Policy - GP 462
14.0 Physical Access for Data Center Policy - GP 463
15.0 Patch Management Policy - GP 464
16.0 Change Management Policy - GP 465
17.0 User Access Management Policy - GP 466
18.0 Information Security and Business Continuity Incident Management Policy - GP 467
19.0 Acceptable Use of IT Equipment Policy - GP 468
20.0 Clear Desk and Clear Screen Policy - GP 469
21.0 Log Management Policy - GP 470
22.0 Data Storage Policy - GP 471
23.0 Database Management Policy – GP 472
Policy Handbook Scope:

This policy applies to the HCT students, staff and any other entity that works at or uses HCT Information Systems (whether on HCT premises or remotely), including all personnel affiliated with third parties all referred in here as the term “Users”. This policy applies to all equipment that is owned or leased by the HCT.

HCT’s IT Security Mission Statement:

“Ensure the Confidentiality, Integrity and Availability of HCT’s information, information systems and the entire network infrastructure against unauthorized disclosure, modification or downtime.”

Objectives:

Information and information systems are considered the foremost important factor in continuing the day to day academic and administrative functions effectively. Supporting the above HCT is committed to secure the information, the information systems and the network infrastructure by adapting to the following principles:

1 - Protect the information and the network infrastructure against external or internal threats.
2 - Provide minimum level of access between information systems and the users on a “Need to- know” basis.
3 - Classify the information according to its criticality to protect it against unauthorized modifications or disclosure.
4 - Adopt set of leading industry standards, guidelines and procedures to ensure the security of information, the information systems and the network infrastructure.
5 - Conduct security awareness campaigns within the HCT about the security policy (i.e. standards, guidelines and procedures) to educate the users about the best security practices when working with information and information systems.
6 - Conduct continuous risk assessment, risk analysis and risk management procedures to information and information systems.
7 - Monitor the logs and audit trails to ensure that information and information systems are protected against unauthorized access.
8 - Ensure that users comply with all UAE federal, local and cyber laws, ethical responsibilities & regulations and information security policy pertaining to information and information systems.
9 - Protect the users and the HCT from any inappropriate use that would expose the HCT to risks including virus attack, compromise of network systems & services and any other legal issues.

**Responsibilities and Undertaking:**

It is the responsibility of the users, who have been provided with the IT services and privileges (such as: Internet Access, Domain user Accounts, Desktop and/or Laptop, E-mail Account, etc.) to make themselves aware of the IT security policy and the sub-policies statements and their responsibilities towards complying with it. Users will be accountable for their actions.

**Compliance:**

Compliance with the HCT’s Information Security Policy is Mandatory for all users. All Users must sign and adhere to HCT Information Security Policy document.

Compliance checks will be performed on a regular basis by the HCT Information Security section.

Any breaches or alleged breaches of this Policy will be investigated in accordance with the current Human Resources and Legal Department procedures and will be directly reported to HR department and the concerned department head to take Disciplinary action.

**Audit and Review:**

The Information Security Section shall review on a regular basis to ensure the policies are enforced.
1.0 Anti-Virus Policy – GP 450

1.1 **Purpose:**

1.1.1 To detect, prevent and minimize the impact of Virus outbreaks in HCT systems such as, servers and end user desktops & laptops.

1.1.2 To protect the systems against the spread of malicious viruses, spyware, malware, Trojans etc.

1.1.3 To define appropriate control measures for users in order to protect the systems against virus attacks.

1.1.4 To ensure protective and optimum performance for the users when using the systems without any considerable delays.

1.2 **Scope:**

This policy applies to all users who have access to HCT information. This includes internal HCT users as well as external parties who receive the information from HCT.

1.3 **Policy:**

1.3.1 **Scanning for Virus:**

1.3.1.1 All files and software downloaded or received from external networks, e-mail, or on any other medium such as data storage media should be first scanned for viruses, malicious code prior to its use.

1.3.1.2 File servers shall be scanned for viruses on a regular basis.

1.3.1.3 Any data storage media brought into the HCT must be scanned for virus before being used by the user.

1.3.1.4 HCT users with institution provided laptop / desktop shall update the Anti-Virus software with latest updates.

1.3.2 **User and Information Security section Responsibilities:**

1.3.2.1 Anti-virus software will be configured to clearly instruct the user to either disinfect or erase the file if a virus is found and users should not disable, remove or change the configuration of the Anti-virus software installed on their desktops and laptops.

1.3.2.2 All users are advised to report virus attacks if any detected to the local IT department.
1.3.2.3 All users are not allowed to open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these emails along with the attachments immediately and then empty the Recycle Bin.

1.3.2.4 All users must delete spam, chain, and other junk email without forwarding.

1.3.2.5 On receiving a virus alert or noticing suspicious activity, users are advised to immediately disconnect their systems from the network and contact local IT department for immediate support.

1.3.2.6 The Information Security section will inform the users regularly of the latest viruses and the precautions to be taken by the users to mitigate the virus risk.

1.3.2.7 E-mail will be used by Information Security section to communicate to the ITAC members about the virus outbreaks and the guidelines to follow as a security precaution. It is Mandatory for users to follow those guidelines.

1.3.2.8 Latest signature updates will be downloaded on to a central server and the updates will be pushed automatically on to the HCT managed desktops and servers with little or no user intervention. This process is scheduled to occur automatically on a daily basis.

1.3.2.9 The Information Security section will regularly check the Anti-Virus server logs to see if all the desktops and servers are running with the latest updates, if not they will manually push the updates.

1.3.2.10 All critical security updates, as soon as they are received from the vendors, will be rolled out to the various desktops, laptops and servers on a high priority basis.
2.0 Password Management Policy – GP 451

2.1 Purpose:

2.1.1 Enforce adequate password controls in systems and at the user level.

2.1.2 Protect information and information assets related to the user.

2.1.3 Ensure that only authorized users can access certain information, applications, services and systems.

2.1.4 Protect the Confidentiality, Integrity and Availability of information, systems, services, and applications within the HCT network.

2.2 Scope:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any HCT facility, has access to the HCT network, or stores any non-public HCT information.

2.3 Policy:

2.3.1 Password Allocation:

2.3.1.1 Every user is given a login ID and a password to access the systems, applications, email, and network resources. The access will be withdrawn when the employee leaves the HCT or if a user’s contract comes to an end or upon request from Human Resource department.

2.3.2 Creating Strong Passwords:

2.3.2.1 The minimum length of a password is 8 characters.

2.3.2.2 User account passwords must not be based on personal information that can be easily guessed or accessed (such as: Based on user name, name of wife, name of husband, date of birth, mobile number, etc.).

2.3.2.3 User account passwords must not be a word in any language, dictionary, slang, dialect, jargon, etc.(such as: password, julie, 123456789, qwerty, etc.).

2.3.2.4 The Password must contain at least one upper case letter (A-Z), one lower case letter (a-z), one numeric character (0-9), or One Special character ( !#^&* ). Password must contain three character sets mentioned in this list. (Example : Bluech1p or Blue#chip).
2.3.3 **Password Expiration:**

2.3.3.1 Passwords will expire after a minimum period of 180 days for normal user accounts and 45 days for privileged user accounts. User accounts with access to ERP system and with system administration capabilities are categorized as privileged users.

2.3.3.2 The new password must be different from your current password and previous two passwords for normal user accounts and previous eleven passwords for privileged user accounts.

2.3.4 **First time Use of Initial Passwords:**

2.3.4.1 A user is assigned an initial password by the HR Office. The user must change this password immediately after the first login.

2.3.5 **Password Reset:**

2.3.5.1 User account password resets will be performed when requested by the user, after verification of identity by HR for staff and student services for student.

2.3.5.2 Where a user has forgotten the password, IT or Student Services department is authorized to reset the password after having the confirmation of the user’s authenticity from HR for staff or from student services department for students. HCT has also facilitated a self-service portal to reset and change password.

2.3.6 **Screen Saver Password:**

2.3.6.1 Every user will use the screen saver with a password, which will be activated within 5 minutes of inactivity.

2.3.7 **Password Protection:**

2.3.7.1 Do not reveal or share your password over phone or email or in person to anyone.

2.3.7.2 Do not hint at the format of the password.

2.3.7.3 Do not reveal your password in questionnaires or Internet.

2.3.7.4 Do not use the “Remember Password” feature of applications (e.g. Outlook, Web-mail, etc.).

2.3.7.5 If you feel that your password is suspected to be compromised, change it immediately.

2.3.7.6 Always lock your computer before leaving your workstation, laptop even for few minutes.

2.3.7.7 Do not respond to any suspicious or untrusted email or Hyper Link with your HCT username and password.
2.3.7.8 User account will be locked out after 10 failed-login attempts for normal users. Privileged user accounts password will be locked out for 1 day after 5 failed login attempts, which can be unlocked only by administrator on the same day.
3.0  Internet Usage Policy – GP 452

3.1  Purpose:

3.1.1 Ensure that the Internet is used for institutional purposes only.
3.1.2 Protect the Information and Information Assets even when users access the Internet.
3.1.3 Communicate within and across HCT network and other departments in a secure manner.
3.1.4 Manage user productivity and optimize the use of IT Infrastructure through control of Internet Access.
3.1.5 Ensure that all users have an efficient Internet access within a secure networked environment.

3.2  Scope:

The Internet usage Policy applies to all users who access the Internet through the computing or networking resources. HCT Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

3.3  Policy:

3.3.1  Internet Access:

3.3.1.1 Internet Access will be provided to the user only after signing and accepting the terms of reference stated in the Internet access form.

https://portal.hct.ac.ae/sites/pnp/hr/Documents/GP038.2_Internet-Access-Form.doc

3.3.1.2 Internet service will be suspended when the staff or student leaves the HCT.

3.3.1.3 Users are permitted the use of the Internet service that supports the institutional needs and for furthering their knowledge in their areas of expertise in the HCT.

3.3.1.4 Users are permitted with limited personal use of the Internet as long as:

a) It does not delay the business/education operations and functions.

b) It does not violate the applicable laws or HCT policy and it does not degrade HCT network performance.

c) Users are not allowed to share their login id and password for accessing internet.

d) Accessing, contributing and downloading from offensive sites are not allowed. Offensive sites include sites that support racism, derogatory religious sentiments, offensive language, defamation, derogatory, abusive attacks on any individual or group and sites having pornographic content.
3.3.1.5 Users are not allowed to use any automated tools or any other means for gaining unauthorized entry into any third party systems or any resource over the Internet to which they do not have authorized access rights.

3.3.1.6 Users are not allowed to engage in any activity that will result in the disruption in operations of either the HCT’s or any third party computer systems.

3.3.1.7 Users are not permitted to post HCT specific, proprietary or confidential information pertaining to the institution on the Internet including forums, groups, Anonymous FTP servers, or any other such open facility.

3.3.1.8 Users are not allowed to use any Chat channels (such as: MSN messenger, Yahoo messenger, or web based chat, etc.) unless they are required for teaching & learning or business purposes.

3.3.1.9 Users are not allowed to download, upload and install software from the Internet. Any such requests will have to be routed to IT department after approval from the concerned Head of Department.

3.3.1.10 Users are not allowed to change the browser settings to use any third party proxy server or external VPN server to connect to internet.

3.3.1.11 The HCT has all the rights to enforce URL filtering to block access to certain sites and limit the bandwidth on certain sites or application that are considered offensive or not relevant to the institution.
4.0 E-mail Usage Policy – GP 453

4.1 Purpose:

4.1.1 Ensure the appropriate method to use e-mail within and across other departments in HCT.

4.1.2 Ensure that risk of exposures of information and information assets are minimized.

4.2 Scope:

This policy covers appropriate use of any email sent from the HCT email address and applies to all users of HCT.

4.3 Policy:

4.3.1 Email Access:

4.3.1.1 HCT’s e-mail access will be provided to the user after signing the internet access Form.

4.3.1.2 The service will be withdrawn when the employee leaves the HCT or if a user’s contract comes to an end.

4.3.1.3 HCT e-mail will be used only for the conduct of the HCT business needs and functions.

4.3.1.4 Ensure that when sending email with the HCT Information and attachments, that the email recipient is the intended person to receive it.

4.3.1.5 Use of e-mail services for purposes constituting clear conflict of the HCT’s functions or in violation of the HCT’s e-mail policy is explicitly not allowed.

4.3.1.6 Use of bcc is not permitted while sending emails. If there is a specific requirement to use bcc, permission should be taken from CTO office.

4.3.1.7 Users are not permitted to use the HCT email to participate in chain letters, e-mails to forward internally or externally.

4.3.1.8 Users are not permitted to send large attachments containing graphics/ pictures/objects/video files that can result in disruption of the HCT’s e-mail services unless if work related.

4.3.1.9 All users must scan and verify that the files to be sent via e-mail as attachments contain no viruses or malicious codes.

4.3.1.10 Unsolicited e-mail/Junk email is to be treated with caution and do not respond to such emails.

4.3.1.11 Usage of profanity, obscenities, or derogatory remarks in any e-mail message is not allowed.

4.3.1.12 Sending emails from another user’s email account is not permitted without written authorization from line Manager, CHRO and CTO.

4.3.1.13 Users are not allowed to send sensitive information to personal email accounts.
4.3.1.14 It is strictly not allowed to use auto forwarding of corporate emails to personal email accounts.

4.3.1.15 Email system is the property of HCT. Access to the mailbox of a departing staff can be provided to another staff for continuity of work upon approval from line manager.

4.3.2 **Virus Protection:**

4.3.2.1 All Incoming/Outgoing e-mails will be scanned for viruses and other malicious content.

4.3.2.2 Gateway Anti-Virus software will be installed on the e-mail server and periodically updated with the latest signatures as and when received from the vendor.

4.3.2.3 The e-mail server will be periodically updated with the latest service packs/patches.

4.3.2.4 Any virus infected e-mail, as detected by the Anti-Virus software and which cannot be cleaned will be quarantined.

4.3.2.5 The sender or recipient will be notified if any viruses are detected in any e-mail and the nature of action taken.

4.3.3 **Mailbox and E-mail size limitations:**

4.3.3.1 Size of email attachment is restricted to 15 MB. Exceptions needs to be done through authorization process and will require approval process of line manager and CTO.

4.3.3.2 Mailbox size for the HCT users will be limited to 1 GB.

4.3.3.3 Requirement of a larger mailbox size will need to go through an approval process of Line Manager and CTO.

4.3.3.4 Users are encouraged to send all attachments to e-mails as a link to share files, for example SharePoint Document.
5.0 Information Classification Policy – GP 454

5.1 Purpose:

5.1.1 Establish a framework for classifying and handling data based on its level of sensitivity, value and criticality to HCT as required by the HCT’s Information Security Plan. Classification of data will aid in determining baseline security controls for the protection of data. A data policy is necessary to provide a framework for securing data from risks including, but not limited to: access, use, disclosure, modification, removal, and destruction.

5.1.2 This policy serves as a foundation for HCT’s data classification security policies, and is consistent with HCT’s data and records management standards. HCT recognizes that the value of its data and data resources lies in their appropriate and widespread use. It is not the purpose of this policy to create unnecessary restrictions to data access or to impede use for those individuals who use the data in support of HCT business or academic pursuits. This policy serves to assure staff and students that the expectation of privacy and confidentiality of their data will be maintained.

5.1.3 All members of HCT community have a responsibility to protect the confidentiality, integrity, and availability of data irrespective of the medium on which the data resides and regardless of format such as, but not limited to: electronic, paper and any other physical form.

5.2 Scope:

This policy applies to all HCT staff and students who access, process, or store sensitive data. This policy applies to all centrally managed HCT enterprise-level administrative data and to all user-developed data stores and systems that shall access HCT data, regardless of the environment where the data resides including, but not limited to: midrange systems, servers, desktop computers, laptop computers, flash drives, and any other mobile computing device. The policy applies regardless of the media on which data reside.

5.3 Policy:

5.3.1 HCT shall classify its data based on its level of sensitivity and the impact to the HCT should that data be disclosed, altered or destroyed without authorization.

5.3.2 All HCT data shall be classified into one of the four classifications:

a) **Confidential Data:** data restricted by law or decided by HCT management as high risk data. Data should be classified as Confidential when the unauthorized disclosure,
alteration or destruction of that data could cause a significant level of risk to the HCT or its affiliates. The highest level of security controls should be applied.

b) **Restricted Data**: data which the Data Owners have decided NOT to publish or make public and data protected by contractual obligations.

c) **Internal Data**: data should be classified as Internal or Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the HCT or its affiliates. All information assets that are not explicitly classified as Confidential or Restricted or Public data should be treated as Internal or Private data. A reasonable level of security controls should be applied to internal data.

d) **Public Data**: data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the HCT and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control should be put to prevent unauthorized modification or destruction of Public data.

5.3.3 HCT Data Owners shall assign a single classification to a collection of data that is common in purpose or function. The most restrictive classification of any of the individual data elements should be used.

5.3.4 HCT’s Information Security section shall protect the confidentiality, integrity and availability of information assets and systems.

5.4 **Roles and Responsibilities**:

5.4.1 **Data Trustees** are senior management or their designates who have planning and policy-level responsibility for data within their functional areas and management responsibility for defined segments of institutional data.

5.4.2 **Data Owners** are managers responsible for the operations and are responsible for appropriately classifying data.

5.4.3 **Data Custodians** are responsible for labeling data with the appropriate classification and applying required and suggested safeguards. The Data Custodian is responsible for implementing the policies and guidelines established by the Data Trustees and Owners. These responsibilities include physical data storage, back-up and recovery, and the operation of security and data management systems etc.
5.4.4 **Data Consumers/Users** are responsible for complying with data use requirements. Data Users also have a critical role to protect and maintain HCT information systems and data. For the purpose of Information Security, a Data User is any employee, contractor or third-party provider who is authorized by the Data Owner to access information assets.
6.0 Bring Your Own Device Policy (BYOD) – GP 455

6.1 **Purpose:**

6.1.1 This policy is relevant to students and third party vendors who use Personally Owned Devices (POD) for their academic or administrative use.

6.2 **Scope**

This policy applies to all students and third party vendors.

6.3 **Policy:**

6.3.1 Access to HCT’s wireless network is provided through authentication using their username and password.

6.3.2 The HCT has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete institution data without reference to the owner or user of the POD.

6.3.3 POD users must ensure that valuable institution data created or modified on PODs are backed up regularly, preferably by connecting to the HCT network and synchronizing the data between POD and a network drive, otherwise on removable media stored securely.

6.3.4 Since IT Helpdesk does not have the resources to support all possible devices and software, PODs used for BYOD will receive a basic or limited support on a ‘best endeavors’ basis for learning purposes only.

6.3.5 POD users are advised to keep their personal data separate from business data on the POD in separate directories, clearly named (e.g. “Private” or “BYOD”).

6.3.6 Students are responsible for bringing a working POD every day to the class with a minimum hardware specification specified by the enrolled program.

6.3.7 POD users must have latest Anti-Virus program running on their laptop with updated signatures before connecting to the HCT’s IT Infrastructure.

6.3.8 POD users must ensure that operating system and other software are updated in real time. This is a critical step because software updates often contain security patches to protect users from the latest threats or exploits.
7.0 Desktop & Laptop Usage Policy – GP 456

7.1 **Purpose:**

7.1.1 Ensure the acceptable use of HCT information systems such as desktop and laptop.

7.1.2 Ensure that if a laptop is lost or stolen, the only impact to the HCT is the loss of the physical laptop asset value and not the valuable information residing on it.

7.1.3 Ensure that employees follow an appropriate level of responsibility to safeguard the desktop and laptop that they have been allocated.

7.1.4 Desktops and Laptops will be issued to the user only after the approval or authorization by the Manager of the concerned department.

7.1.5 The Desktop and Laptop will be withdrawn when the employee leaves the HCT or if a user’s contract comes to an end or upon a request from the Manager of the concerned department.

7.2 **Scope:**

This policy applies to the use of all HCT IT resources (e.g., desktop computers, laptops, printers, disk space storage, software, telecommunications equipment, networks, Internet, E-mail, etc.) and supporting infrastructure that is owned, leased, or controlled by HCT and used by its staff and students.

7.3 **Policy:**

7.3.1 Users must safeguard their Desktop against any damage.

7.3.2 Users must safeguard their Laptop against loss, theft or damage.

7.3.3 Users must not leave their Laptops unattended even for few minutes for example, in public area, airports, etc.

7.3.4 Users must lock their account when leaving the Desktop and/or Laptop unattended.

7.3.5 Users must ensure that the Corporate Anti-Virus program is updated on their Desktop and/or Laptop all the time.

7.3.6 Staff are not allowed to connect their personal Laptops to the HCT network.

7.3.7 Users must be careful to safeguard Information Assets when accessing the IT Infrastructure from a public place.

7.3.8 Users must backup their institution related files that they store on their Desktop or laptop on a regular basis on their SharePoint folders.
7.3.9 Users must not tamper with the administrative functions of the Desktop or Laptop such as its Operating System or Administrator identification and password.

7.4 **Terms and Compliance:**

7.4.1 Information Security section must ensure that the Desktop, Laptop build and implementation confirms to the minimum requirements.

7.4.2 All users who are issued with a Desktop or Laptop are responsible to safeguard the device and any stored Information assets on it.

7.4.3 In the event of loss of a Laptop, users must report the loss to the police in the country where the loss occurred and must contact the Information Security section or local IT department as soon as possible to limit the access to HCT systems.

7.4.4 The Information Security section or local IT department must investigate the circumstances of the loss of Laptop before a replacement is issued to the user.

7.4.5 Compliance with this policy is mandatory for all users with a desktop or laptop.
8.0 Software Compliance Policy – GP 457

8.1 Purpose:
8.1.1 This policy defines standards for use of company and third party software. This policy addresses software licensing, copyright and usage security requirements for all the users.

8.2 Scope:
This policy applies to all HCT Students, Staff, contractors, vendors and agents. This policy covers all software’s that are either purchased or in-house developed for operating within HCT.

8.3 Policy:

8.3.1 Software Licensing:
8.3.1.1 Purchase and use of third party software must be in accordance with third party licensing agreements.
8.3.1.2 Specific user restrictions such as the number of copies allowed to be installed, the number of desktops, laptops and servers the software can be installed on, or the number of concurrent users of the software allowed at one time must be in accordance with the license purchased.
8.3.1.3 The use or copying of purchased software so that it can be used on a computer other than the computer for which it is licensed is strictly not allowed.
8.3.1.4 Users are not allowed to install any software prior to the approval and authorization of the Manager of the concerned department and the approval of Information Technology department.
8.3.1.5 The duplication of the software media or documentation is not allowed.
8.3.1.6 The Information Security section will perform periodic reviews of software used on the HCT desktops, laptops and servers to ensure that it is in compliance with licensing agreements.
8.3.1.7 All software found in violation will be removed immediately. Individuals responsible for downloading or using non-compliant software on the HCT system will be subject to disciplinary actions.

8.3.2 Software Copyrights:
8.3.2.1 All users of software on the HCT systems must strictly abide by the “Copyright Laws” and restrictions detailed by the software manufacturer.
8.3.3 Use of Shareware and Freeware:

8.3.3.1 Many freeware and shareware programs are available on the Internet and other locations. Most of these programs are legitimate and perform their advertised functions properly. Some of these programs are ineffective, inefficient, not secure, and include malicious code to harm the systems or the network. Most users are not capable of evaluating the performance or security of the programs. Therefore, Information Security section reserves the rights to either approve or disapprove the software requested for the freeware and shareware to be used on the HCT’s systems and network.

8.3.4 Software Ownership:

8.3.4.1 Computer software developed by or for the HCT is the sole property of the HCT.

8.3.4.2 This policy must be conveyed to all third parties who develop software or applications for the HCT’s use. This prevents dispute about ownership of the software, including the source code, once the project is complete. Software developed by the HCT’s employees on HCT time becomes the property of the HCT.

8.3.4.3 Any Software or Application that are purchased or developed within HCT needs Chief Technology Officer’s written approval before publishing them internally or over the internet.
9.0 Back-up and Restoration Policy – GP 458

9.1 Purpose:
The objective of Backup and Restoration policy is to recover the information and information systems from an unplanned business disruption that could cause damage to its integrity, confidentiality or availability.

9.2 Scope:
This policy pertains solely to electronic data stored in the HCT network devices hosted in main data center and disaster recovery data center. Data custodians are responsible for providing adequate backups to ensure the recovery of electronic information (includes HCT Records and software) in the event of failure.

9.3 Policy:

9.3.1 Backup Requirements:

9.3.1.1 Backup requirements for all information and information systems within the HCT must be identified and documented.

9.3.1.2 The Information Security section will record and maintain the backup requirements for all systems under the responsibility of IT at a minimum, this will include details of backup frequency, information to be backed up, storage media, retention and recycling.

9.3.1.3 In the case of data stored locally on desktops/laptops, it will be the responsibility of the users to ensure that the data is backed up on a periodic basis. Users wishing to backup their data, shall either transfer data onto their network drive folders or request the IT department to make a backup on suitable data storage media. Such requests will require specific authorization by the concerned Head of Department.

9.3.1.4 The IT department will decide which information is to be backed up and the frequency of backups in consultation with the information owner based on the system criticality and it’s Recovery Time.

9.3.2 Backup Schedule:

9.3.2.1 All systems software, application software, user data, database information and associated documentation, will be backed up on a regular basis to facilitate recovery in the event of an unplanned system disruption. The frequency of the backup will be at a minimum:
a) System Software: Before and after any changes to systems such as an upgrade, changes in configuration, patch updates etc.

b) Application Software: Before and after any changes to the application such as a new version release or modification to application source code.

c) User Data or Database Information: On a periodic basis (Daily / Weekly / Monthly), based on the backup frequency identified for the individual systems.

d) Device Configurations: Before and after any changes to the configurations of critical devices such as Routers, Firewalls, switches etc.

e) Documentation: Latest copies of system documentation (e.g. Technical reference manuals, User manuals etc.) will be backed up and maintained.

9.3.3 Performing backups:

9.3.3.1 IT department will maintain a weekly backup checklist specifying the various backups that are required to be taken for that day.

9.3.3.2 The weekly backup operations will be logged against the checklist reviewed and signed off by the assigned engineer at the end of the day. At a minimum, the backup log will record details about the backup carried out, start and end time, identification of the media used and success or failure status.

9.3.3.3 Any unscheduled or one-time backups will require specific authorization by the concerned head of department. This will also be recorded in the daily backup list with appropriate reasons for the same.

9.3.3.4 The backup checklist will be independently reviewed by Head of Information Systems and Technology Department periodically.

9.3.4 Backup storage:

9.3.4.1 Backup media will be stored in two different locations - one onsite within the HCT’s premises, and the other at a location set by the HCT.

9.3.4.2 Physical access to the backup media will be adequately secured by implementing appropriate controls.

9.3.4.3 Physical access to the backup storage locations will be restricted only to authorized personnel.

9.3.4.4 A physical access log will be maintained for recording access to the backup storage locations. This will be reviewed on a periodic basis by Head of Information Systems and Technology Department.
9.3.4.5 Backup media will be stored in an environment that is adequately protected from fire, dust and humidity, magnetic interference etc.

9.3.5 **Tape Storage:**

9.3.5.1 All backup tapes are to be labeled using a bar-coding system. Barcode will contain the following information.

a) Job Name  
b) Creation Date and Time  
c) Backup Type (Incremental, Differential or Full)

9.3.5.2 Weekly, monthly tapes will be stored off-site physical location in a fire-proof cabinet.

9.3.6 **Age of Tapes:**

9.3.6.1 The first date of each tape that was put into service shall be recorded on the tape. Tapes that have been used longer than two years shall be discarded, destroyed and replaced with new tapes.

9.3.7 **Media and Restoration Management:**

9.3.7.1 The IT department will maintain an up to date inventory of all backup media within the HCT. This will include details such as Media identification, Data contents, Physical location, Start date of usage, number of tape writes etc.

9.3.7.2 All backup media will be clearly labelled and classified to ensure that they are easily identifiable and maintain the HCT’s information classification policy.

9.3.7.3 The IT department will carry out a physical verification of the media inventory at least every six months. Media due for disposal will be identified in advance and a report will be generated for the same, which will be circulated to the respective system owners for approval.

9.3.7.4 All backup media will be disposed of in a secure manner at the end of their life. It will be ensured that:

a) The media is properly degaussed;  
b) Labels/tags containing reference to the HCT internal information are removed;  
c) Tapes and other non-reusable data storage media are physically destroyed.

9.3.7.5 Data on backup media will be restored at least once in every 6 months to verify the recoverability of data.
9.3.8 Testing and Restoring:

9.3.8.1 The ultimate goal of any backup process is to ensure a restorable copy of data exists on the backup tapes or backup media. As a result, it’s essential to regularly restore the data from backup tapes or backup media. Full restore will be performed according to the annual restore plan. These plans will be reviewed by Information Security engineer on a regular basis.

9.3.8.2 Data will be restored if:

a) There is a compromise of the system / device.

b) Files have been corrupted, deleted, or incorrectly modified but try to recover.

c) The Information to be accessed is located in an archive backup.

9.3.8.3 In the event a data restore is desired or required, the following policy will be adhered to:

a) An approval from the data owner is needed for any restoration process.

b) An approval from CTO is also required for any restoration process.

9.3.8.4 In the event of a local data loss due to human error, the affected end user shall contact local IT helpdesk and request a data restore.
10.0 Remote Access Policy – GP 459

10.1 **Purpose:**

10.1.1 Define standards for connecting to the HCT’s network from any remote host.

10.1.2 Minimize the potential exposure to the HCT systems which shall result from unauthorized use of its resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

10.2 **Scope:**

This policy applies to all HCT staff, students, contractors, vendors and agents with a HCT-owned or personally-owned computer or workstation used to connect to the HCT network. This policy applies to remote access connections used to work on behalf of HCT, including reading or sending email and viewing intranet web resources.

10.3 **Policy:**

10.3.1 **User Responsibilities:**

10.3.1.1 It is the responsibility of the users with remote access privileges to the corporate network to ensure that their remote access connection is given the same consideration as the user’s on-site connection to the HCT.

10.3.1.2 The user is responsible to ensure no one violates any of the organizations policies, does not perform illegal activities, and does not use the access for outside business interests of HCT when accessing the corporate network remotely. The user bears responsibility for the consequences should the access be misused.

10.3.1.3 Users with remote access privileges must ensure that their organization-owned or personal computer or workstation, which is remotely connected to HCT’s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

10.3.1.4 At no time should any user provide their login or email password to anyone, not even family members.

10.3.1.5 Users with remote access privileges to the HCT’s corporate network must not use non-corporate email accounts (i.e., Hotmail, Yahoo, AOL, etc.), or other external resources to
conduct the HCT’s business, thereby ensuring that official business is never confused with personal business.

10.3.1.6 Personal device that is used to connect to the corporate network must meet the requirements of the organization-owned equipment for remote access.

10.3.1.7 All hosts that are connected to the corporate network via remote access technologies must use the most up-to-date anti-virus software and patched appropriately, this includes personal computers.
11.0 Wireless Communication Policy – GP 460

11.1 **Purpose:**

11.1.1 The purpose of this policy is to set the standard for network operation and security, specifically in the context of wireless network access. The configuration, installation, and maintenance of wireless communication network access point devices, if unmanaged, could result in severe interference with other network users and serious security risks. Information Technology department define the standards for the use of networks, including the wireless communications spectrum on campuses.

11.1.2 This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the HCT network. Only those wireless infrastructure devices that meet the standards specified in this policy are granted to connect to HCT network.

11.2 **Scope:**

This policy applies to all HCT staff, students, contractors, vendors and agents who connects to HCT wireless network using any mobile device. This policy also applies to all wireless infrastructure devices that are connected to HCT network or reside on HCT site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting wirelessly.

11.3 **Policy:**

11.3.1 Use HCT configured authentication protocols, username and password for connecting to wireless infrastructure.

11.3.2 Wireless infrastructure devices that provide direct access to corporate network must:

   a) Enable Wi-Fi Protected Access Enterprise (WPA2.Enterprise) protocol. It also must use Advanced Encryption standard (AES) with minimum of 128-bit key length.

   b) Be configured to change the default SSID name.

   c) Be configured with password protected SSID.

   d) Be configured with firewall feature sets on the Wi-Fi controller to protect inter user communication and college IT assets.

11.3.3 HCT guests shall be provided with username and password to gain access to network.
12.0 Mobile Phone Policy – GP 461

12.1 **Purpose:**

12.1.1 The purpose of this policy is to describe the rules covering the use of mobile computing devices that can be attached to HCT networks, or containing HCT Information.

12.2 **Scope:**

HCT allows usage of mobile phones as part of normal business processes. However, care needs to be taken over their use, and of the data that they hold. Information Processing Equipment, Intranet and e-mail access provided by the HCT is intended primarily for HCT institutional use, but limited access of personal use is allowed.

12.3 **Policy:**

12.3.1 All HCT supplied mobile devices and their contents remain the property of HCT and are subject to regular audit and monitoring.

12.3.2 Users must be aware that the device contain HCT data, and take appropriate action to protect the device from being lost or stolen. Users must configure password to lock the screen.

12.3.3 Once received, the user is not authorized to change any security device settings without reference to the IT helpdesk, as they shall affect the security of the device.

12.3.4 Devices eligible for this dispensation are limited to smart phones, blackberry or PDA’s which include iOS / Android / Windows devices. These devices must have their security settings (such as passwords) configured.

12.3.5 If the information you carry has been classified as HCT Confidential, then this information should not be carried on mobile devices unless it is encrypted (where this facility is available on the device and where it is not, the user must consider carefully before allowing it to be stored on the device).

12.3.6 Phones enabled with cameras should primarily be used for taking business/education related pictures. However, some limited personal use is allowed, but storage must not interfere with HCT institutional use.

12.3.7 Users shall only take pictures of individuals with their permission to do so.

12.3.8 Information stored on a mobile device should be downloaded to a secure device (HCT Laptop for example) and removed from the phone at the users’ earliest opportunity.
13.0 Dispose of Media Policy – GP 462

13.1 **Purpose:**

13.1.1 All storage media will be physically or magnetically destroyed permanently before disposal. This will be performed by Information Security engineer, or by official agents on their behalf. In the case of an external company being used to destroy media on a large scale, then “certificates of secure destruction”, must be obtained. In the event of magnetic media being taken off-site by third party, these contractors must be bound by a confidentiality agreement.

13.1.2 Where the equipment or media are to be used again by other staff or outside the HCT, a secure overwriting of previous data must be performed. All items disposed of (whether sold/removed/destroyed) must be documented accordingly by recording the asset numbers in the IT hardware asset inventory. The disposal of IT equipment should be authorized by the HCT disposal committee.

13.2 **Scope:**

The scope of this policy includes all electronic media in the HCT and all personnel who are responsible for or who use HCT computer systems. Vendors and contractors who have access to the HCT computer systems are also subjected to this policy.

13.3 **Policy:**

13.3.1 Confidential waste paper products shall be stored separately from ordinary paper waste for recycling.

13.3.2 All such waste must be shredded before removal from HCT premises.

13.3.3 The confidential waste shall only be removed by authorized persons.

13.3.4 Confidential waste should be securely stored and not left in corridors or outside awaiting removal.

13.3.5 Confidential waste shall not be used for any other purpose either before or after it has been shredded, for example, as scrap paper or packing material.

13.3.6 Any digital storage media to be disposed of must be securely wiped.
14.0 Physical Access for Data Center Policy – GP 463

14.1 Purpose:
14.1.1 The objective of this policy is to establish rules for accessing the Datacenter, disaster recovery site and network rooms.

14.2 Scope:
This policy applies to the HCT Data Center and other Server Room facilities operated by IT at the HCT.

14.3 Policy:

14.3.1 Access to Data Center:
14.3.1.1 All doors of the Data Centers, Network Rooms and DR site shall be closed at all times. Access mechanism shall be in place.
14.3.1.2 Any access to the data center shall be logged (in and out, accessing ID, reasons, authorized by whom). In addition, all accompanying persons shall be listed.
14.3.1.3 Authorization and approval to access the data center shall be provided by the operations staff in either email or paper.
14.3.1.4 Any non-HCT staff accessing the datacenter shall be accompanied by authorized employees from HCT at all time.
14.3.1.5 Visitors are not allowed to bring phones or computer, except they have permission from operation’s manager.
14.3.1.6 Access to data center and network rooms during an emergency, should be approved by CTO.

14.3.2 Monitoring the Access
14.3.2.1 Any access and activity inside the datacenter shall be recorded.
14.3.2.2 CCTV shall be working and recording all motions in the datacenter.
14.3.2.3 Windows to the datacenter have to be clear all the time, to be able to watch the people inside the datacenter.
15.0 Patch Management Policy – GP 464

15.1 Purpose:

15.1.1 All operating systems and applications need regular patching to ensure their continued security and reliability. If patches are not applied on time, this might permit hackers to compromise a computer, which, in turn, threatens all computers and networks connected to it. Therefore, any computer equipment that runs an operating system or application and is connected to the HCT network shall have up-to-date security patches applied.

15.2 Scope:

This policy applies to workstations or servers owned or managed by HCT. This includes systems that contain company or students data owned or managed by HCT regardless of location.

15.3 Policy:

15.3.1 Vulnerability assessments shall be performed by Information Security section and according to the results, system patching shall be performed by HCT IT department. This should apply to all servers, desktop, handheld, and laptop computers, network and security devices inside the HCT network.

15.3.2 All hardware and software, servers, desktop and laptop including components, shall be accurately listed in the HCT asset inventory to aid in patching efforts.

15.3.3 In addition to the Vulnerability assessment scanning, the Information Security engineer shall regularly check the Web for newly released information about vulnerabilities. This shall include using the information sent by HCT alerting solution.

15.3.4 The Information Security section shall assess each vulnerability alert prior to taking any action in order to avoid unnecessary patching.

15.3.5 The decision to apply a patch, and within what timeframe, shall be done as presented in the patch priority matrix below.

15.3.6 All patches shall be downloaded from the relevant vendors or other trusted sources. Each patch’s source shall be authenticated and the integrity of the patch verified. All patches are submitted to an anti-virus scan upon download.

15.3.7 New servers and desktops network and security shall be fully patched upon coming online by the IT infrastructure department and deployed in order to limit the introduction of risk.
15.3.8 The IT department shall develop a list of vendors whose patches are trusted and are applied without test. All other patches shall be tested prior to implementation. A server should be designated to serve as a test bed for newly released patches with a test period of below matrix before issuing live patches to the production network.

15.3.9 A rollback plan that allows safe restoration of systems to their pre-patch state is devised prior to any patch rollout in the event that the patch has unforeseen effects.

15.4 **Patching Priorities:**

15.4.1 The following patch (Microsoft & Operating System) priority matrix represents all systems at HCT, their relative priority for vulnerability patching, and timeframes within which patches must be applied.

<table>
<thead>
<tr>
<th>System</th>
<th>Criticality</th>
<th>Duration for Medium – Low patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstations/Laptops</td>
<td>Medium</td>
<td>4 Weeks</td>
</tr>
<tr>
<td>DNS/Domain Controller</td>
<td>High</td>
<td>6 – 8 Weeks</td>
</tr>
<tr>
<td>Servers providing web servers</td>
<td>High</td>
<td>6 – 8 Weeks</td>
</tr>
<tr>
<td>Mail Servers</td>
<td>High</td>
<td>6 – 8 Weeks</td>
</tr>
<tr>
<td>Antivirus server</td>
<td>High</td>
<td>6 – 8 Weeks</td>
</tr>
<tr>
<td>Network appliances</td>
<td>High</td>
<td>6 – 8 Weeks</td>
</tr>
<tr>
<td>Other servers &amp; appliances</td>
<td>Medium</td>
<td>6 – 8 Weeks</td>
</tr>
<tr>
<td>Network and Security devices</td>
<td>High</td>
<td>6 – 8 Weeks</td>
</tr>
</tbody>
</table>

All critical security updates related to HCT services will be tested and deployed at the earliest of its release. To mitigate any such zero day vulnerability, network security devices like Firewall. Next Generation Intrusion Prevention System will be configured to block malicious traffic.
16.0 Change Management Policy – GP 465

16.1 **Purpose:**

16.1.1 Ensure change requests comply with HCT change management procedures.

16.1.2 Publish a calendar that specifies the “maintenance window” (when changes will be allowed) and network availability.

16.1.3 Eliminate or reduce the number of errors related to change planning and change implementation.

16.1.4 Implement changes as per schedule.

16.1.5 Provide a back out plan for all changes.

16.1.6 Ensure the changes do not affect warranty services.

16.2 **Scope:**

This policy provides direction related to the application of change management for all IT Applications, Server, and Infrastructure devices supporting HCT internal and perimeter networks and applies to all staff and students at HCT.

It covers all HCT’s Enterprise Applications, data networks, network and security devices, LAN servers and personal computers (stand-alone or network-enabled), located at HCT campuses and operational sites, where these systems are under the jurisdiction or ownership of the HCT, as well as any personal computers, laptops, mobile devices and or servers authorized to access the HCT’s data networks.

16.3 **Policy:**

It is the responsibility of the Information Systems and Technology Department to manage the life cycle of all IT systems supporting HCT operational activities related to teaching and learning, administrative and technical support. To ensure effective change management within the HCT’s Information Technology environment, following shall apply:

16.3.1 Under no circumstances shall any entity integrate new applications into a production environment without approval from CTO office.

16.3.2 All proposed types of changes that shall impact HCT’s Information Resources must adhere to this Change Management Policy.

16.3.3 No change shall be made to HCT IT environment without the approval of Change Advisory Board. (CAB)
16.3.4 All changes shall follow the established approval process to ensure that changes are completed with minimum restrictions and risk.

16.3.5 All changes shall be well documented for future reference.
17.0 User Access Management Policy – GP 466

17.1 Purpose:

17.1.1 The purpose of this policy is to prevent unauthorized access to the information systems and to ensure the availability of information for authorized users. The policy describes the registration and de-registration process for all information systems and services.

17.2 Scope:

This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices. Such information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally.

17.3 Policy:

17.3.1 New Users:

17.3.1.1 Access to applications, databases, network, email and servers are controlled through a formal user registration process beginning with a formal notification from HR (for employees), Student / Academic Services for students and department heads (for temporary engagements). Each user is assigned a unique user ID in order for users to be identified and held accountable for their activities.

17.3.1.2 The use of shared IDs is only permitted where they are suitable for the work carried out (i.e. Training).

17.3.1.3 Based on the user’s department management request, users will be provided with standard IT services (e.g. shared folders, applications, remote access & network services).

17.3.1.4 A request for service must be submitted (email or hard copy) by the new user’s line manager or by HR. Login credentials will be only handed to the users, on the first day of their joining. IT will maintain a record of all new user requests on the service desk. Users will be granted privileges on the basis of their job responsibilities and roles.

17.3.1.5 Temporary accounts shall be created based on the approval for third party consultants or contractors. Requesting department should provide identity details like Passport to HR for the creation of temporary user credentials.
17.3.2 Change in User Responsibilities:
17.3.2.1 Changes in user access shall be triggered by their respective line manager and shall be implemented by work flow process.

17.3.3 Reset of Password:
17.3.3.1 Where a user has forgotten the password, IT or Student Services department is authorized to reset the password after having the confirmation of the user’s authenticity from HR for staff or from student services department for students. Automatic password reset options are available for users through self service portal.

17.3.4 Removal of Users:
17.3.4.1 User access to all services will be disabled at midnight on the last working day by IT processes, once HR marks last working day for an employee.
17.3.4.2 IT Department is responsible for reviewing all user access rights every month in HCT domain controller.
17.3.4.3 IT Department will coordinate with respective owner at the applications in order to disable user’s access on applications.
18.0 Information Security and Business Continuity Incident Management Policy – GP 467

18.1 Purpose:

18.1.1 The purpose of this Policy is to prevent security incidents, limit the damage if an incident occurs, awareness of Information Security related issues and to improve HCT IT process to serve the business effectively at HCT. This policy also addresses handling of incidents that might cause a disturbance to business continuity. The Incident Management Policy applies to all the users of HCT.

18.2 Scope:

This policy applies to all HCT staff and students.

18.3 Policy:

18.3.1 Information Security Incident Practices:

18.3.1.1 It is the responsibility of all students and staff of HCT to promptly report Information Security incidents as defined in this policy.

18.3.1.2 The local IT department within HCT shall be responsible for overseeing the incident handling processes at the HCT.

18.3.2 Business Continuity Incident Practices:

18.3.2.1 It is the responsibility of all staff of HCT to promptly report business continuity incidents to the local IT helpdesk by phone or email.

18.3.3 Information Security Incident Handling:

18.3.3.1 The local IT department shall serve as a focal point in HCT for computer security incident reporting and response.

18.3.3.2 The local IT department shall handle computer security incident reports and provide assistance in recovery actions.

18.3.3.3 All Security Incidents shall be prioritized based on the Criticality of the affected assets, Current and potential technical impact of the incident.

18.3.3.4 A Security Incident Response Procedure shall be defined within HCT with the steps to be followed in case an incident occurs.
18.3.3.5 Escalation Procedure shall be defined to escalate the incident to management and relevant parties to ensure that important decisions are promptly taken.

18.3.3.6 Procedures shall be developed, documented and updated to record any security breach, whether accidental or deliberate.

18.3.3.7 Whenever a Security breach occurs each incident shall be logged, assigned for follow-up, analyzed, recommendation shall be made in respect of prevention.

18.3.3.8 Local IT Department shall be responsible for auditing the incidents on periodic basis and ensure that preventive action process is in place to address such further incidents.

18.3.3.9 Local IT Department shall ensure that adequate details relating to software malfunctions (Security related malfunctions) are recorded and the actions to be followed are implemented.

18.3.3.10 Security review and audit of all IT systems shall be conducted on a regular basis to promptly identify any possible security loopholes and/or areas of improvement to the system.

18.3.3.11 Appropriate disciplinary action against individuals who caused the incident shall be initiated.

18.3.4 Business Continuity Incident Handling:

18.3.4.1 The Information Security section is responsible for handling all business continuity incidents.

18.3.4.2 The Information Security section is responsible for ensuring that personal safety takes priority.

18.3.4.3 Upon receiving notification of or observing an incident, The Information Security section shall:

   a) Take action to verify all details that have been reported;
   b) Evaluate this information against the criteria for activation of the business continuity plan;
   c) Notify emergency contacts and apply appropriate information dissemination;
   d) Ensure safe site evacuation, if required;
   e) Mobilize safety, first aid or evacuation-assistance department;
   f) Identify root causes of the event;
   g) Limit the damage of the business continuity event;
   h) Management of media contact;
   i) Collect information, logs, reports etc. about the incident, as much as possible;
   j) Close the incident;
k) Review incident logs at least once per month to identify trends and avoid re-occurrence.

18.3.4.4 The Information Security section shall ensure awareness of users and compliance with the Business Continuity Plan.
19.0 Acceptable Use of IT Equipment Policy – GP 468

19.1 Purpose:
19.1.1 The purpose of this policy is to outline the acceptable use of HCT computing equipment and IT infrastructure services at HCT. Inappropriate use exposes HCT to risks including virus attacks, compromise of network systems and services, and legal issues.
19.1.2 The intentions for publishing the IT Acceptable Use Policy are not to impose restrictions that are contrary to HCT but to establish a culture of openness, trust and integrity. HCT is committed to protecting HCT’s users, partners and the HCT from illegal or damaging actions by individuals, either knowingly or unknowingly.

19.2 Scope:
This policy applies to students and staff at HCT. This policy applies to all IT equipment and IT Services that are owned or leased by HCT.

19.3 Policy:

19.3.1 Acceptable Use and Ownership:
19.3.1.1 Users shall report any suspicious activity observed on HCT’s Information systems to the Information Security section immediately.
19.3.1.2 HCT’s Information Security engineer reserves the right to check networks and systems on a periodic basis to ensure compliance with IT Security policy.
19.3.2.3 Software installations on the desktop/laptop computers shall be in compliance with the enlisting approved and supported software and services.
19.3.2.4 Operating System and Applications must be continuously updated with latest patches / service packs.
19.3.2.5 Only authorized personnel shall have access to information stored on Intranet servers and shared folders.
19.3.2.6 Classified data and files shall be maintained in accordance with Information Classification Policy.
19.3.2.7 The removal of property including data, hardware or software shall be with the relevant custodian authorization and as per dispose of media policy.
19.3.2.8 Email received from unknown senders, with or without attachment shall not be opened and deleted immediately.

19.3.3 **Handling Proprietary, Confidential and Private Information:**

19.3.3.1 HCT has classified its information as defined in the Information Classification Policy, that includes but is not limited to company private, competitor sensitive or research data, corporate strategies, trade secrets, specifications and students lists.

19.3.3.2 HCT would like to ensure the safeguard of its information assets at all times and that employees will take all necessary steps to prevent unauthorized access to this information;

19.3.3.3 Authorized users are responsible for the security of their passwords and accounts.

19.3.3.4 All PCs, laptops and servers should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes.

19.3.3.5 Information contained on portable computer is vulnerable, special care should be exercised.

19.3.3.6 All computers used by the employee that are connected to the HCT Internet / Intranet / Extranet, shall be continually executing approved virus-scanning software with a current virus database as per Malicious Code and Antivirus Policy.

19.3.3.7 Personal laptops or computing devices of staff shall not be connected to HCT local wired or wireless network.
20.0 Clear Desk and Clear Screen Policy – GP 469

20.1 **Purpose:**

20.1.1 The purpose for this policy is to establish a culture of security and trust for all employees at HCT. An effective clean desk effort involving the participation and support of all HCT employees can greatly protect paper documents that contain sensitive information about our students, clients, customers and vendors. All employees should familiarize themselves with the guidelines of this policy.

20.1.2 The main reasons for a clean desk policy are:

a) A clean desk can produce a positive image when our customers or third party vendors visit HCT.

b) It reduces the threat of a security incident from confidential information being leaked away when left unattended.

c) Sensitive documents left in the open can be stolen by a malicious entity.

20.2 **Scope:**

During known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.

At the end of the working day the employee is expected to tidy their desk and to put away all office papers. HCT shall provide lockable desks and filing cabinets for this purpose.

20.3 **Policy:**

20.3.1 Always clear your workspace before leaving for long periods of time.

20.3.2 Consider scanning paper items and filing them electronically in your workstation.

20.3.3 Use the shredder for documents when they are no longer needed.

20.3.4 Lock your desk and filing cabinets at the end of the day.

20.3.5 Lock away portable computing devices such as laptops or Mobile phones.

20.3.6 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
21.0 Log Management Policy – GP 470

21.1 **Purpose:**

21.1.1 Logs are records of events that occur within the information systems. Virtually every system, service, application and device in the Enterprise has built in logging capabilities. Originally log data was used to troubleshoot systems; but as systems and business/education requirements evolved, so did logging capabilities and log analysis. In today’s Enterprise, logs are an invaluable resource used to optimize systems and networks, establish baselines, perform audits and assist with regulatory compliance.

21.1.2 System logs for operating systems and services, such as authentication, file and print, DNS, email, and so forth, generate detailed information about their activity. Application logs have the ability to generate an audit trail of past transactions with time stamps, user names and object access details. Most network devices, such as firewalls, routers, switches, and so forth, have the ability to generate log data about their activity.

21.1.3 Change management logs document all changes made to technologies used within HCT. Other types of logs, such as surveillance or physical access logs provide detailed physical access audit trails. Each of these logs sources are an integral part of their respective administrators jobs because the collection and analysis of the log data is one of their responsibilities.

21.1.4 In conjunction with the appropriate tools and procedures, audit trails can validate individual accountability, a way to reconstruct events, detect intrusions, identify problems and demonstrate regulatory compliance. The need to audit individual accountability, reconstruct events, detect intrusions, identify problems and demonstrate regulatory compliance emphasizes the need for organizations to develop an effective log management strategy to generate, analyze, store and dispose of log data.

21.2 **Scope:**

This policy applies to all HCT systems, network, databases and applications used to establish and support a production environment.

21.3 **Policy:**

21.3.1 Information Security engineer shall create, maintain and Implement a secure log management infrastructure by balancing system performance, storage resources, and legal requirements;
21.3.2 Commit resources to perform timely log review to identify and analysis access, change monitoring, malfunction, resource utilization, security events and user activity;
21.3.3 Identify roles and responsibilities of staff associated with this process;
21.3.4 Develop standards, procedures, and guidelines as needed to support this program;
21.3.5 Make the system available for applications that need log management and analysis capabilities.
21.3.6 The system should log: User ID, Dates and times of logon and logoff, terminal identity (if possible) and Network address (if possible), unsuccessful system or data access attempts (if possible), System alerts or failures or other significant events as appropriate.
21.3.7 Special treatment should be performed for administrator, developer, super-user or other privileged access.

21.4 **Log Retention:**

21.4.1 Log retention has to be done according to legal requirements, targets, guidelines and security policies from HCT.

21.4.2 In the course of running different services on the server a number of logs are collected, like Web Logs, Email Logs, System Services Logs, Applications Logs and Security Logs. These logs can take many different formats e.g. Text, Word, Excel and Notepad Files, Email Format.

21.4.3 Many of the above documents can be retained as ‘hard’ paper records or in electronic form. Retention of specific documents shall be necessary to:

a) Fulfill statutory or other regulatory requirements.

b) Provide Evidence for an events/agreements in the case of disputes.

c) Meet operational needs.

d) Ensure the preservation of logs of historic or other value.

21.4.4 Conversely, the permanent retention of all logs is undesirable, and appropriate disposal is to be encouraged for the following reasons:

a) There is a shortage of storage space.

b) Disposal of existing logs can free up space for more productive activities.

c) Indefinite retention of personal data shall be unlawful.

d) Reduction of fire risk (in the case of paper records).
21.5 **Logs Retention and Protocol:**

21.5.1 Logs should be enabled for Operating Systems, Applications, Firewall, Switches and other security devices in the data center as defined in the log management policy.

21.5.2 Logs should be saved locally on the devices, logs are collected for the period of one week, after which logs will be transferred to centralized network storage.

21.5.3 The entire log should be reviewed by log mining tools for any malicious activity or at least manually once a year.

21.5.4 The retention period for the logs should be 1 year.

21.5.5 After the completion of retention period logs should be disposed securely.

21.5.6 Information Security engineer is responsible to handle all the issues related to logs.

21.5.7 Log can be used to address performance issues for the servers, applications, firewall, router or other devices.

21.5.8 Log deletion should be authorized by the CTO, where computer files are concerned.

21.5.9 Paper records related to logs must be shredded on site with the approval of CTO.
22.0 Data Storage Policy – GP 471

22.1 **Purpose:**

22.1.1 This policy will assure network data storage is used in an acceptable manner to maintain network availability and performance. Infrastructure department is responsible for managing network storage which includes daily backups, securing access, monitoring, and reporting of usage patterns. Access and use of network storage establishes an obligation on the part of the individual to use this resource as defined in this policy.

22.2 **Scope:**

This policy applies to all HCT students, staff, third party and vendors who access, process, or store sensitive HCT data.

22.3 **Policy:**

22.3.1 **Appropriate File for Storage:**

22.3.1.1 Files that directly pertain to the business of HCT shall be saved on a server. These include business files created through the use of HCT approved and installed software.

22.3.1.2 Users are not allowed to store any personal or non-business related files on storage server.

22.3.2 **Storage Space Allocation:**

22.3.2.1 Alerts will be sent to all employees who are close to exceeding their server space quota. If an employee exceeds their server space quota, they will be unable to save files until sufficient allocated space is freed in order to accommodate them. If an employee needs support in freeing storage space, he or she shall contact the local IT department.

22.3.3 **Tips for Conserving Storage Space:**

22.3.3.1 It is the responsibility of every user to ensure that they use their server storage space allocation wisely. Each user should set aside time on a monthly basis to ensure that they remain within their space quota. Identify, remove and/or archive items that are:

a) Outdated, such as preliminary draft versions of current documents.

b) Out-of-use or orphaned files.

c) Duplicated files.

d) Non-business related or non-critical files.
23.0 Database Management Policy – GP 472

23.1 Purpose:

23.1.1 The database management policy establishes methods for protecting databases from accidental or malicious destruction of data or damage to the database infrastructure.

23.2 Scope:

This policy applies to all HCT databases, related appliances and applications used to establish and support production, test, and disaster recovery environments.

23.3 Policy:

23.3.1 Default service account passwords such as SYS and SYSTEM must be changed after creation. All default operating system account passwords including ROOT must be changed.

23.3.2 Database administrators shall have the operating system privileges to create and delete files in the production servers. Access to non-production database servers must be approved by CTO.

23.3.3 Each database service account is managed by a single employee. During vacations and emergencies, these accounts must be delegated to other users temporarily based on CTO approval.

23.3.4 All database user account access must be approved by the CTO. The approval should include the requesting department manager, data owner, and CTO. The access for all accounts must be reviewed once every quarter to ensure users have access as per their current job role.

23.3.5 No database user accounts associated with an employee shall have direct privileges to update, create or delete records in the production databases. Database Roles (based on job title and responsibilities) should be used to manage the privileges available to users.

23.3.6 All database user accounts will be associated with a password policy as per the industry standards.

23.3.7 Data auditing mechanisms must be in place to investigate in case of unauthorized activities on the database.

23.3.8 Live production systems data must be updated from the relevant front-end applications by the appropriate authorized users. Any scripts or backend changes to production databases must have approvals from data owner and CTO.
Roles and Responsibilities:

Head of IT Security:

1. Ensure that all aspects of this policy are implemented and operational in all relevant system components.
2. Periodically review all relevant activities as mentioned in the policy.
3. The logs should be reviewed by Head of IT Security every Quarter.

Information Security section:

1. Periodically monitors and reports all issues and relevant activities to Head of IT Security and Infrastructure Department all relevant activities.
2. Assists the Head of IT Security in reconciling audit trail anomalies, the logs should be reviewed by Head of IT Security every Quarter.
3. Reports security breaches or anomalies to the Head of IT Security and Infrastructure Department.
4. Will coordinate with Information Security engineer for incident reports or update.
5. Review all the proposed changes related to security before the stake holders, for example network admins implement the changes.

Information Security Engineer Role:

1. Prepare and maintain policy guidelines on monitoring and audit trail recording, protecting, reviewing and reporting.
## IT Security Policy Task Force

<table>
<thead>
<tr>
<th>S/N</th>
<th>Name</th>
<th>Position</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Saif Bamadhaf</td>
<td>Chief Technology Officer</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Varghese PV</td>
<td>Senior Manager, IT Services</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Khalid Tariq</td>
<td>Head, Enterprise Systems Development</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Abdelghafour Al Ali</td>
<td>Information Security Engineer</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Saifudheen Veedu</td>
<td>Network Engineer</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Anvaj Aliyarukutty</td>
<td>Infrastructure Analyst</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Sabeena KM</td>
<td>Business System Analyst</td>
<td></td>
</tr>
</tbody>
</table>
Glossary:

- **Access**: Access refers to the act of obtaining or using any given information, or entering an information processing facility. It shall also refer to the very right to perform the act.
- **Access control**: Access control is a mechanism to enable authorized people to access entity resources (physical and logical) while preventing unauthorized people from doing the same.
- **Access Point**: An access point is a device that allows wireless communication devices to connect to a wireless network using standard wireless networking protocols (e.g. 802.11).
- **Access privileges**: Access privileges refer to the level of access granted to a user to perform his/her job duties.
- **Accountability**: Accountability means that people are responsible for their action. This can be achieved through audit trails and non-repudiation.
- **Antivirus**: Anti-virus is software used to prevent, detect and remove virus or malware on desktop, laptops, servers or any other computing equipment/devices.
- **Assets**: Assets are economic resources. It is anything tangible or intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value.
- **Audit Trails**: A security-relevant sequential record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.
- **Authentication**: Authentication is the act of verifying a claim of identity. It is usually one or more of the following: something you know (password), something you have (identification card) or something you are (finger print).
- **Availability**: Part of the Information Security Triad; availability means that information should be available when it is needed.
- **Awareness**: Awareness is the knowledge and attitude members of an entity possess regarding the protection of the physical and, especially, information assets of that entity. Many entities require formal
security awareness training for all workers when they join the entity and periodically thereafter, usually annually.

- **Backup**: Backup refers to the technique of making copies of data so that these additional copies shall be used to restore the original data after a data loss event.

- **Business Continuity Plans (BCP)**: Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an entity will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.

- **Business impact**: Business impact is defined as the damage implications that are caused by an event. Business Impact analysis looks at whether that impact is acceptable by the stakeholders or not.

- **Change**: Is defined as any alteration to original software, hardware, or other aspects of the data processing environment and its attached networks.

- **Change Advisory Board (CAB)**: A CAB is a group of people that approves changes to HCT’s Information Technology Environment.
  
  The CAB department consists of the following people:
  - Deputy Vice Chancellor - Administration (or designee),
  - Chief Technology Officer (or designee) and
  - Appointed members of Change Management Department.

- **Change Driver (CD)**: The Change Driver is the individual facilitating the change management process. This person assumes full responsibility for coordination and documentation of changes to the production environment. The Change Driver also assumes responsibility for scheduling and communicating the change to all appropriate work groups.

- **Change Management**: Change management is a formal process for directing and controlling alterations to the information processing environment. The objectives of change management are to reduce the risks posed by changes to the information processing, environment and improve the stability and reliability of the processing environment as changes are made. The change management process ensures that a change is: Requested Approved, Planned, Tested, Scheduled, Communicated, Implemented, Documented and Reviewed after the change.

- **Change Management Department (CMT)**: A CMT is a group of people nominated to research, implement and manage change in HCT Information Technology environment and who assist the change management process in the assessment, prioritization and scheduling of changes.

Members of this committee include
This department assures quality, validates the test plan and processes related to the change whilst identifying and mitigating risks factors that shall arise from proposed production changes.

- **Classification**: Classification means assigning categories to assets on pre-set criteria. In Information Security classification is used to categorize information assets in terms of sensitivity to protect it from unauthorized access, use, disclosure, disruption, modification or destruction.

- **Clear Screen**: Clear Screen is a control, where all users are enforced to avoid leaving their computers/laptops without being logged off. This ensures that the contents of the computer screen are protected from prying eyes and the computer is protected from unauthorized use.

- **Clear Desk**: Clear Desk is a control to ensure that all HCT staffs clear their desks at the end of each work day. This not only includes documents, ID Cards and notes, but also post-its and removable media (CDs, floppy disks, memory sticks).

- **Confidential Data**: Generalized term that typically represents data classified as confidential, according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.

- **Computer Devices**: refer to both desktop and laptop provided by the HCT to users which help them in fulfilling their job obligations effectively.

- **Compliance**: Compliance is the act of adhering to, and demonstrating adherence to, a standard or regulation (international or internal).

- **Confidentiality**: Part of the Information Security Triad; confidentiality means the non-disclosure of certain information assets expect to an authorized person as per the classification level of that asset.

- **Configuration management**: Configuration management is an IT service management process that tracks all the individual configuration items (IT Assets) in an IT system with shallbe be as simple as a single server or an entire IT department.
- **Copyright:** Copyright, a form of intellectual property law, protects original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture, etc.

- **Credentials:** User ID, Passwords or any other official identification that confirms somebody’s position or status.

- **Custodian:** A custodian is defined as an individual or entity that has approved responsibility for maintaining an information asset.

- **CTO:** Chief Technology Officer.

- **Database Service Account:** Accounts created in the database for database administration and application-specific data or access management.

- **Database User Account:** User Accounts created in the database which are associated with a person.

- **Encryption:** Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

- **Evidence:** Evidence is everything that is used to determine or demonstrate the truth of an intrusion or breach to an information system.

- **Third Party:** Individual or Entity having contractual agreement/obligations or legal agreement/obligations or business obligations to provide services to the HCT. Commonly referred as Second Party or Third Party.

- **Framework:** A framework is the combination of guidelines and structured processes that address a complex issue. The framework establishes policies and practices to provide general guidance on matters affecting Information Security.

- **Incidents:** An incident can be thought of as violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

- **Information:** Depicts any government related information, which can exist in many forms, such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

- **Information Assets:** any information or information processing facility that has value to the HCT.

- **Information Processing:** Information processing entails any activity on the information including, but not limited to, creation, modification, deletion, storage, transmission, replication, encryption, decryption, etc.

- **Information Resources (IR):** Includes any hardware or software that makes possible the storage and use of data.
- **Information Security**: The act of protecting information that shall exist in any form, whether spoken, written, processed or transmitted electronically, etc. from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities.

- **Information Security Section**: individuals selected from each department / section to support the implementation of IT Policy in the HCT.

- **IT Sections**: These are the different operational groups within the IT department,
  - Business Solutions;
  - Information Systems;
  - IT Infrastructure;
  - Information Security.

- **Information Security Incidents**: Refers to known or suspected, single or series of unwanted or unexpected Information Security incidents/events that have or shall have a significant probability of compromising business operations at the HCT. Additionally, it refers to the act of violations or suspected violations of the Information Security policies/procedures/standards at the HCT.

- **Information Assets**: Definable pieces of information in any form, recorded or stored on any media that is recognized as “valuable” to the University

- **Information systems**: Any computerized system used for managing and processing any government related information within a single entity or crossing multiple entities.

- **Integrity**: Part of the Information Security Triad; integrity means that data cannot be modified without authorization, intentionally or unintentionally.

- **Inventory**: Inventory is a list of goods and material owned by an entity - inventory recording could be in the form of an asset register.

- **Institutional Data**: All data owned by the HCT

- **Intellectual Property**: Intellectual Property refers to any creations that are legally protected. Intellectual property includes copyrights, trademarks, trade names, and logos of the HCT.

- **Key**: Key is a piece of information or a parameter that determines the functional output of a cryptographic algorithm or cipher. Key is used to de-crypt the encrypted information or data.

- **Laptop**: also known as notebooks, are portable computers that are small in size and weight and can be carried from one place to another, and include a battery which allows them to operate without being plugged into a power outlet.
- **Logs**: stream of messages in time-sequence often comprises a log. Logs are generated by network, security devices, operating systems, applications and any computing device.

- **Malware**: Malware is software used or created to disrupt computer operation, gather sensitive information, or gain access to computer systems.

- **Media**: refer to Electronic media where data are stored in digital form. (e.g. hard disk drives).

- **Mobile Devices**: Portable or handheld devices that can store and process data, via mobile data service and/or Wi-Fi connectivity that allow users to access information remotely, such as smartphones, Personal Digital Assistants (PDAs) and tablet computers (excluding laptop computers) and include both official mobile devices provided through the HCT and personal mobile devices if connected to the HCT network or its infrastructure.

- **Non-public Information**: Any information that is classified as Internal/Private Information according to the data classification scheme defined in this document.

- **Patch**: A Patch is a piece of software designed to fix problems or improve the usability and performance of a system.

- **Patch Management**: a process to manage the deployment of patches to a large number of information systems in an HCT.

- **Policy**: An Information Security related document written and maintained to provide governing statements regarding any Information Security key process, through setting the rules for expected behavior by users, systems administrators, management, and security personnel; authorize security personnel to monitor, probe, and investigate; define and authorize the consequences of violation; define the entity consensus baseline stance on security; help minimize risk; and help track compliance with regulations and legislation.

- **Procedure**: An Information Security related document; adjunct to policy and written to give step-by-step directions on ‘how’ of carrying out the policy statements.

- **Recovery**: Data recovery is the technique of recovering data from the backed up media in the event of loss or failure of data in the information processing systems.

- **Regulatory**: Regulatory refers to the use of rulemaking, monitoring and enforcement of rules by the state.

- **Remote Access**: The ability to connect to and access the HCT Infrastructure from a remote location using the virtual private network (VPN) of the HCT.

- **Removable Media**: Removable media refers to portable storage media which are designed for storing information and easily detachable from the computers. Examples include: Optical discs (Blu-ray discs,
DVDs, CDs), Memory cards (Compact Flash card, Secure Digital card, Memory Stick), Floppy disks / Zip disks, USB (universal serial bus), Disk packs, Magnetic tapes, Paper data storage (punched cards, punched tapes).

- **Request for Change (RFC):** A request for change can be initiated from any source, and shall be in response to management decisions, requirements of business stakeholders, or requests from the CTO and department heads.

- **Retention period:** Retention period is the period for which an information / data needs to be stored and maintained before disposing it in a secured manner.

- **Risk:** Risk is the quantifiable likelihood of potential harm that shall arise from a future event.

- **Risk assessment:** Risk assessment is a step in the risk management process to determine the qualitative and quantitative value of risk in relation to a recognized threat. Quantitative risk assessment requires calculations of two components of risk; R, the magnitude of the potential loss L, and the probability that the loss will occur.

- **Security breach:** A Security breach is an act that bypasses or contravenes security policies, practices or procedures.

- **Security control:** Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks. They could be preventive, detective or corrective.

- **Senior management:** Senior Management: A layer of management in an entity whose primary job responsibility is to monitor activities of subordinates as well as the day to day operations; for example Managers/Directors of HR, IT, Finance, Marketing, engineering, etc. while reporting to upper management such as CEO or Director General.

- **Sensitive Data:** Generalized term that typically represents data classified as Confidential according to the data classification scheme defined in this document.

- **Services:** Refers to the HCT’s internal or external, IT or non IT, services provided to individuals or businesses or government entities.

- **Spyware:** Spyware is a type of malicious software installed on computers that collects information about users without their knowledge.

- **SSID:** Service Set Identifier (SSID) is a unique name set to a wireless local area network (WLAN) for the purpose of identification.

- **Statutory:** A formal written law of a legislative authority that governs a state, city, or country.

- **System Administrator:** An individual or group of staffs responsible for the maintenance, operation and administration of the information systems.
- **Technical / Functional Lead:** The person implementing the change

- **Threat:** Threat is the expressed potential for the occurrence of a harmful event such as an attack. It could be any party with the intent and capability to exploit vulnerability in an asset such as a malicious hacker or a disgruntled staff.

- **User:** User is an individual, including staffs (permanent & contracted staffs) and non-staffs (contractors, consultants, suppliers, vendors, partners, customers, etc.) Users of the HCT, who has access to the information and information processing facilities of the HCT and uses it for their day to day activities.

- **User ID:** A name used to gain access to a computer system.

- **VPN:** A virtual private network or VPN is a network that uses a public network, such as the Internet, to provide remote offices or individual users with secure access to their HCT’s network in a cost-effective manner.

- **Vulnerability:** Vulnerability is weakness in an asset that can be exploited.

- **Work Groups (WG):** Work Groups consist of stakeholder representatives identified by the Information Technology Service Department and are responsible for implementing changes assigned to them.

- **WPA2:** Wi-Fi Protected Access is a security protocol for wireless local area networks (WLANs) defined in the 802.11i standard. WPA2 has replaced WPA. WPA2 implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.