THE UNIVERSITY OF THE WEST INDIES
Information Security Policy Guidelines

These guidelines have been produced to assist members of the University community and those using University of the West Indies (UWI) ICT facilities to secure UWI information assets. These guidelines complement UWI's Information Security Policy and should be read in conjunction with it.

1. General

These apply to all users within the University community.

1.1 Do not let others see your computer keyboard or screen when you are typing your username and password or when you are processing sensitive data.

1.2 If you need to leave the computer temporarily, take your memory stick and other materials with you and lock the computer, that way no one will be able to see your username and password or read your files. If you cannot take the materials you should lock them away.

1.3 Before you print materials on a shared printer, make sure you know where the printer is located. Collect your printouts as soon as possible. Lock the computer before collecting your printouts.

1.4 When using web-based services, ensure that the data is encrypted on the site. The data on the site is encrypted if *https://* appears in the address bar and a lock icon displayed (at the bottom of the screen or to the left of the https://)

1.5 Persons who handle confidential information should not allow anyone to be in the proximity where information can be easily seen or read.

1.6 There should be multiple authorized personnel assigned to access information. This will allow the availability of information irrespective of the authorized handler.

1.7 Information classified as confidential that is retrieved form any system in editable format should be secured by authorized personnel. This can be done using passwords to restrict access to the document.

1.8 Passwords *(Appendix I has additional details on selecting strong passwords)*

1.8.1 Use strong passwords and keep them safe.

Passwords should not be the same as the user ID and be at least six characters, and contain at least one alpha and one numeric character, e.g. "pr0t3ct1on". *(Be sure to contact CITS at your campus for the minimum password requirements at your campus.)*

1.8.2 Change your password at least once per academic year.

1.8.3 Do not use the same password in succession.

1.8.4 Never send your password to <u>anyone</u> in an email.

1.8.5 Never save your password in a web browser.

1.8.6 Never save passwords or use “Remember Me” options on a public computer.

1.8.7 Never write down your password.

1.9 E-Mail

1.9.1 E-mail attachments may be infected with malware. Beware of all unusual e-mails and especially e-mail attachments. Do not open suspicious e-mails

1.9.2 Use caution with e-mails. The sender of an e-mail may be someone other than the person whose name shows up in your inbox. Viruses may also send e-mail without any user action.

1.9.3 Oftentimes unsolicited advertisements and chain letters are spam. Delete them immediately. Do not answer such emails or forward them to other users. You should only forward these when making a report to the CITS at your campus.

1.10 The Internet

1.10.1 Data transmitted over the internet is often insecure. Be careful to ensure that sensitive data are not transmitted via the internet unless by way of a trusted VPN connection.

2. Staff

In addition to the General Guidelines (above), the following should also be considered by members of staff.

2.1 Your staff username and password should be used by you alone. Not even IT staff should know your password. ***You are responsible for all activities carried out under your username.***

2.2 If the IT Helpdesk provides you with a new password, change it immediately to a password that you alone know.

2.2 Staff wishing to create shared resources on their computers should consult a CITS representative or personnel with delegate by a relevant IT authority.

2.3 Some staff have proximity or smart Id cards for identification purposes and for accessing restricting areas. As the owner of the card, you are responsible for the use of your smart card, therefore:

- ensure that you have your proximity or smart Id card on you at all times;
- do not lend your proximity or smart Id card to others – even fellow staff members;
- do not use your proximity or smart Id card to admit others – even fellow staff members – to restricted areas.

3. Students

In addition to the General Guidelines (section 1), the following should also be considered by students.

3.1 The University, through CITS, assigns each student a user name and password for accessing UWI systems. Immediately change the password from the initial one provided by CITS to one that is only known by you. ***You are responsible for all activities carried out under your username.***

3.2 When you send an email, ensure that you know the correct email address of the recipient. Check the email address for typographical errors before sending the email.

3.3 Be cautious about sharing your University assigned email address with persons on the internet or in internet fora. Consider registering for a free email address (Hotmail, Gmail, etc.) using a pseudonym and fictitious address for use in internet for Social networking (Facebook, MySpace, etc.)

4. Custodians of IT Systems (usually IT staff)

4.1 Encrypt data stored on UWI equipment: Encryption is essential to protecting sensitive data and to help prevent data loss due to theft or equipment loss. Ensure that data (both at rest and in-transit) and file systems are encrypted.

4.2 Encrypt data stored in the Cloud: Many cloud applications do not encrypt by default. Check and managing the security settings on the public cloud services that handle data

4.3 Use digital certificates to sign all of your sites: Obtain digital certificates from one of the trusted authorities and save these to devices other than web servers (as is traditionally done).

4.4 Have A Plan For Replacing Breached Certificate Authorities: Digital certificates are vulnerable to fraud, and must be replaced when compromised. Develop a management process to ensure business continuity by quickly replacing a compromised certificate and its accompanying encryption keys.

4.5 **Use Appropriately Strong Encryption Keys:** Find out what the latest recommended key strength is and use it to encrypt data.

4.6 **Rotate SSH Keys Annually:** This should be done to ensure that staff who leave do not have remote access to critical infrastructure.

4.7 **Implement Data Loss Prevention (DLP) and auditing:** Use data loss prevention and file auditing to monitor, alert, identify, and block the flow of data into and out of your network.

4.8 **Implement a removable media policy:** Restrict the use of USB drives, external hard disks, thumb drives, external DVD writers, and any writeable media. These devices facilitate security breaches coming into or leaving your network.

4.9 **Secure websites against MITM and malware infections:** Use SSL, scan your website daily for malware, set the Secure flag for all session cookies, use SSL certificates with Extended Validation.

4.10 **Use a spam filter on email servers:** Use a time-tested spam filter such as Spam Assassin to remove unwanted email from entering your users' inboxes and junk folders. Teach your users how to identify junk mail even if it's from a trusted source.

4.11 **Use a comprehensive endpoint security solution:** Symantec suggests using a multi-layered product (theirs, of course) to prevent malware infections on user devices. Antivirus software alone is not enough. Antivirus, personal firewall, and intrusion detection are all part of the total approach to endpoint protection.

4.12 **Network-based security hardware and software:** Use firewalls, gateway antivirus, intrusion detection devices, honey pots, and monitoring to screen for DoS attacks, virus signatures, unauthorized intrusion, port scans, and other "over the network" attacks and attempts at security breaches.

4.13 **Maintain security patches:** Some antivirus programs update on what seems like a daily basis. Be sure that your software and hardware defences stay up to date with new antimalware signatures and the latest patches. If you turn off automatic updating, set up a regular scan and remediate plan for your systems.

4.14 **Educate your users:** The most vulnerable element in any network is almost always the human element. An informed user is a user who behaves more responsibly and takes fewer risks with valuable University data, including email.

4.15 **Shared Printers**: There may be several printers that exist on the network that hare of the same type and model. To prevent users from being assigned the wrong printer, the share name should be changed so the suitability of CITS and access groups created to use shared printers.

5. Campus IT Services (CITS)

Campus IT Services is the generic description for the department on each campus that provides information technology and related services to the campus, (and UWI affiliated units at that campus). All centre departments are affiliated with a campus and are therefore serviced by the CITS unit at the campus with which it is affiliated. Below is a list of and contact information for all UWI CITS.

Campus	**Campus-specific Name**	**Contact**
Cave Hill	Campus IT Services (CITS)	**Email:** itservicedesk@cavehill.uwi.edu https://livesupport.cavehill.uwi.edu https://reset.cavehill.uwi.edu (Self Service Password Reset) **Service Desk Line:** (246) 417-4191 (Staff Support) (246) 417-4595 (Student Support)
Mona	Mona IT Services (MITS)	• Telephone Support : (876) 927-2148 or extensions 2740, 2739, 2992 or Digicel lines (876) 618-6466/618-6469/473-9358 • Electronic Support: helpdesk@uwimona.edu.jm • Phishing email contact : phishing@uwimona.edu.jm
Open	Computing and Technical Services (CATS)	• **Telephone:** (868) 663-8155 • **Fax:** (868) 645-9741 • **Email:** cats@open.uwi.edu
St Augustine	Campus IT Services (CITS)	**Service Desk** Email: servicedesk@sta.uwi.edu Dell PC Orders Email: pcorders@sta.uwi.edu Webmaster: webmaster@sta.uwi.edu

		Telephone: 1-(868)-662-2002 ext. HELP (84357)

Appendix I – Selecting a Strong Password

The weakest link in your information security chain is usually your password. Unfortunately, with the advance in password-cracking techniques, the traditional advice for creating passwords no longer holds. A password created with that advice, like ***jal43#Koo%a****,* is very easy for a computer to break and very difficult for a human to remember and type.

The following was provided by WordPress.com (http://en.support.wordpress.com/selecting-a-strong-password/).

There are many different approaches to generating a strong password, but password managers and passphrases are the best. Choose the one that works for you, and then read its corresponding section further along in this article to learn how to get started.

Best: Use a Password Manager – A password manager is a software application on your computer or mobile device that generates very strong passwords and stores them in a secure database. You use a single passphrase to access the database, and then the manager will automatically enter your username and password into a website's login form for you.

You never have to worry about choosing a good password, remembering it, or typing it again. This is the easiest and most secure method available today, and we strongly recommend that you use it.

Good: Create a Pass*phrase* instead of a Password - A passphrase is similar to a password, except that it's based on a random collection of words, rather than just one. For example, ***copy indicate trap bright****.*

Because the length of a password is one of the primary factors in how strong it is, passphrases are much more secure than traditional passwords. At the same time, they are also much easier to remember and type.

They're not as strong as the kinds of passwords generated by password managers, but they're still a good option if you don't want to use a password manager. They're also the best way to generate the master password for a password manager or your operating system account, since those can't be automatically filled in by the password manager.

How to Create a Passphrase

Creating a passphrase follows similar rules to creating a traditional password, but it doesn't need to be as complex, because the length of the phrase will provide enough security to outweigh the simplicity.

1. Choose 4 random words.
2. Add spaces between the words if you prefer.

At this point, you should have something that looks like: ***copy indicate trap bright***

You can stop there if you'd like, or you can add some extra strength by following these steps:

1. Make a few of the letters upper-case.
2. Add in a few number and symbols.

After applying those rules, it will look something like: ***Copy indicate 48 Trap (#) bright***

Things to avoid:

- Don't place the words in a **predictable pattern** or form a proper sentence; that would make it much easier to guess.
- Don't use **song lyrics, quotes or anything else that's been published**. Attackers have massive databases of published works to build possible passwords from.
- Don't use any **personal information**. Even when combined with letters and numbers, someone who knows you, or can research you online, can easily guess a password with this information.