CCBRT

INFORMATION AND COMMUNICATION TECHNOLOGY

ICT USAGE POLICY SUMMARIZED

TERMINOLOGY

ABBREVIATION	DEFINITION
ICT	Information technology & communication
I&BA	Innovation and Business Analysis
SLA	Service Level Agreement
Version	1.4

Table I Abbreviations

ICT USAGE POLICY SUMMARIZED (The DO's & DON'T's)

Scope:

This policy applies to all staff, consultants, Guests and volunteers at CCBRT who use the organization's Information, Communication & Technology resources.

INTERNET USE

DO's

1. Use the internet service to support productive work activities. Example performing work related researches.
2. Use the Guest Wireless network to access internet on personal mobile devices such as mobile phones and tablets
3. Apply for internet access / special site access by completing the IT.05 Internet Access Request Form where required.

DON'T's

1. Knowingly attempt to gain access to restricted website and/or systems
2. Knowingly access websites and/or systems that have been compromised with viruses or any potentially damaging applications.
3. Disclose or share your access credentials with others
4. Disclose someone else's access credentials
5. Access or attempt to access inappropriate content. Inappropriate contents include pornography, racial or religious slurs, gender specific comments, terrorism, information encouraging criminal skills or material relating to cults, gambling and illegal drugs
6. Take part in any activities on the internet that could bring CCBRT into disrepute
7. Create or transmit material that might be defamatory or incur liability for CCBRT
8. Use internet for any illegal or criminal activities;
9. Send offensive or harassing materials to others;
10. Broadcast unsolicited views on social, political, religious or other non-business related matters;
11. Send or post messages or materials that could damage CCBRT's image or reputation.
12. Abuse the provided internet access by excessively downloading large files which may affect the overall internet experience.

EMAIL USE

DO's

1. Use your ccbrt.org corporate email account for all official work related communication.
2. Always log out from your email account after use;
3. Use strong password to enhance the security of your email account;
4. Avoid setting obvious passwords example your name, date of birth
5. Routinely change your password for better security;
6. Routinely check your email account for new emails and respond at a reasonable time.
7. Set an "out of office message" to communicate your absence to the sender when you are on leave/not available to respond to mail for an extended period of time.
8. Report suspicious emails of unknown senders before attempting to open them
9. Ensure the emails you send out have a signed sender name and information at the end.

DON'T's

1. Misuse the "Reply All" functionality. "Reply All" functionality should only be used when all recipients in the email chain are required to see the communication;
2. Download attachments and/or files from suspicious unknown senders
3. Attempt to open/read emails from suspicious unknown senders.
4. Use personal email account for official work related communications.
5. Tamper with security and email scanning software.
6. Access another user's company email account. If they require access to a specific message (for instance while the employee is off or sick), they should approach their line manager who in turn will communicate to the I&BA department with such request;
7. Share email account credentials, and specifically passwords.
8. Write or send emails that might be defamatory or incur liability for the company
9. Create or distribute any inappropriate content or material via email
10. Use email for illegal or criminal activities;
11. Send offensive or harassing emails to others
12. Send messages or material that could damage CCBRT's image or reputation.
13. Use CCBRT email services to run commercial activities (Except as specifically offered by CCBRT management)
14. Leave their email account unattended/unutilized for an extensive period of time.

ICT ASSETS USE

DO's

1. Always ensure your provided ICT assets are safely secured (as advised by I&BA Personnel) while on and out of office environment.
2. Keep laptops, workstations and other ICT machines away from excessive heat, wet and dusty environment
3. Portable ICT assets such as Laptops and tablets must be physically and logically locked when unattended.
4. Properly switching off machines when not in use;
5. All requests for new or change of application/system software must be presented to the I&BA unit with clear user requirements as instructed by I&BA;
6. All purchase of ICT related equipment must pass through I&BA department, for instance organization software and licenses and other ICT related hardware and software;
7. All changes that impact or require involvement of ICT infrastructure should be discussed and approved by the Head of I&BA unit;
8. Recycle bins should be emptied regularly;
9. Computers should be free from dust and water and should therefore be cleaned by a dry cloth regularly;
10. Ensure you have a valid gate pass for your ICT assets before attempting to leave the CCBRT premises with them.

    Note: ICT asset gate passes can be requested via completing the IT07. ICT Gate pass access request form.
11. Shutdown your workstation and/or device every after use

DON'T's

1. Leave portable ICT assets Example Laptops, mobile phones and tablet unattended and unsecured, whether on or out of office environment.
2. tamper with or rearrange how equipment is plugged in (computers, printers, projectors, power supplies, network cabling, modems, etc.) without first consulting I&BA department;
3. Remove or attempt to remove the asset tags marked on the CCBRT ICT Assets.
4. Attempt to gain access or compromise securely identified areas (such as server rooms)
5. Tamper with or attempt to tamper with firewall and antivirus systems that are installed and maintained across the entire CCBRT network to ensure security;
6. Attempt to leave with CCBRT ICT assets without prior authorization or valid gate pass.

TELEPHONE USE

DO's

1. Answer your phone in a polite and professional manner
2. Hang up the phone by returning the receiver on the correct position on the phone every after you complete a phone call
3. Periodically check to ensure phone is placed in the correct position and the receiver is well placed.
4. Use you're provided pin code to make outside work related calls only.
5. Introduce yourself and department in the initiation of every telephone conversation.

DON'T's

1. Use loud speaker to answer the phone unless communication involves other individuals in the room
2. Knowingly/ purposefully unplug your desk phone.
3. Intentionally forward calls to other extensions without prior agreement and/or communication with the other impacted party.
4. Use harsh tone or language while communicating via the phone.
5. Share provided pin code with other individuals.

DATA USE

DO's

1. Store personal data separately from organizational data (as instructed by I&BA unit)
2. Always ensure your data is saved properly and at the correct location as instructed by the I&BA unit.

DON'T's

1. Save personal files, such as videos/songs/pictures on the Desktop, My documents, shared folder and work folders, these areas are specific for work related materials only
2. Store excessively personal data on CCBRT workstations to the point that it compromises the performance of the device.
3. Disclose Organizational data to unauthorized individuals and/or third party.
4. Attempt to access restricted and/or unauthorized data systems.
5. Spawn unauthorized data sources. I&BA unit is the sole custodian of data systems.
6. Falsify or forge extracted/ obtained data from data systems

Declaration

I have read and understood the terms and conditions of this policy, I hereby agree to adhere and abide to policies stated within.

Full name: ____.

Job title: ____.

Department: ____.

Signature: ____.

Date: ____.