MCIC ICT POLICY

ICT Guide lines and Procedures

MAY 28, 2018

OTR ICT DIVISION

MCIC BETIO TARAWA

Table of Contents

Table of Contents 1
MCIC Information & Communication Technology (ICT) Policy 2
A. Main Task 2
B. System Requirement 2
C. Email Server 3
D. Users Responsibility 3
E. Internet Access (Surfing) 3
F. Laptop and Desktop Policy 6
G. Server Privilege User 6
H. Sever Shared Drive 6
I. ICT Division Right 6
J. Damage and Lost of ICT Equipment 6
ICT Guide Lines 7
K. New Computer Setup 7
L. Add a New Email User 8
M. Adding a new Domain User 9

MCIC Information & Communication Technology (ICT) Policy

The ICT Division within the Ministry of Commerce, Industry and Cooperatives (MCIC) will be responsible for all support and services as follow:

A. Main Task

1. Overall monitoring the network within the MCIC, inbound and outbound access for staff
2. Administration right of the ICT Department on all Hardware and Software of the MCIC.
3. Maintenance for all computers and laptops.
4. Stock or Inventory Control of all hardware and software.
5. Maintenance for Printers, Scanners and photocopier if the supplier of the hardware cannot fix it due to their warrant agreement.
6. Overseeing and recommend proper use of ICT Hardware and Software
7. Overseeing any intrusion from inside and outside the office for virus, Trojans and worms infectious.
8. Monitoring the email server.
9. Ensuring that Privacy of data were maintain and certainly create rules that automatically assign right for each staff.
10. Monitoring the use of the internet within the office to be utilize with official use only.
11. Monitoring the use of the computers for official use only.
12. Backup data at all times
13. Given the recommendation and proper ICT equipment for procurement process for the MCIC.
14. Monitoring and administrator to the FingerTec

Given the above task, the following classified in details.

B. System Requirement

I. All Laptops should have a following minimum requirement:
   a. Hard drive capacity of 300GB
   b. CPU Core of i5
   c. RAM of 4GB
   d. 64bit Processor
   e. Brand: Dell Latitude only

II. All Computers (PC) should have the following minimum requirement
   a. Hard drive capacity of 500GB
   b. CPU Core of i3
   c. RAM of 8GB
   d. 64bit Processor
   e. Brand: Dell only

III. If the above I & II requirement not meet by the local supplier, then the following will apply
   a. Hard Drive capacity 500GB
   b. CPU Core i5
   c. Ram of 8GB
   d. 64 bit processor
   e. Brand: Lenovo, Acer or HP

C. Email Server

I. Staff should only use their official email (commerce.gov.ki) for correspondence and not allow to use their personal email from Yahoo, Gmail etc.
II. Staff using the MCIC email to send inappropriate content to other staff within and outside of the MCIC, their email will be disable immediately.
III. All staff should report their travel to overseas in case that their email can be access or hack while at overseas, so the ICT will monitor their email.
IV. Staff should change password and report any error or technical issues with their email to the ICT Officer.
V. Sharing password between staff is not allowed.
VI. ICT Officer will disable the accounts temporary if there is a threat that report from the email server.

D. Users Responsibility

I. All computers should be properly shut down by the users.
II. All staff not allowed to bring the MCIC Laptop and others to their homes, unless there is an authorisation from the Director of each centre or the Secretary.
III. Officer that authorise to bring their Laptop and others ICT Hardware to their homes will responsible for the lost and damage of the equipment unless there is a report from the police for the theft and damage.
IV. Users are prohibited to use the CDs or DVDs on their computer to play and burn movies and music.
V. Playing games on the computer are not allowed, games software will be remove by the ICT Officer.
VI. All staff are not allowed to drink and eat on their tables and in front of their computers and Laptops.
VII. All staff are not authorise to lend their computer to other people outside of the MCIC for their used.
VIII. Staff are not allowed to do their Private matter on the MCIC Computers.
IX. Copying any data from the MCIC Shared drive is strictly prohibited.
X. All staff should clean their computer or laptop and other ICT devices monthly.
XI. Private computers will not be allowed to connect to the MCIC network unless authorise by the SRO for Ministry of Commerce, Industry and Cooperatives.
XII. Private computers that connect to the MCIC Network will follow the policy guideline and procedures.

E. Internet Access (Surfing)

I. Strictly prohibited to browse the following Categories:
- **Abortion** – Web pages that discuss abortion from historical, medical and legal
- **Alcohol** – Web pages that promote, advocate or sell alcohol including beer, wine and hard liquor
- **Anonymizer** – Web pages that promote proxies and anonymizers for surfing websites with the intent of circumventing filters
- **Atheism & Horoscopes** – Web pages that pursue an anti-religion agenda or that challenge religious, spiritual, metaphysical, or supernatural beliefs

- **Auctions & Marketplaces** – Web pages devoted to person to person selling or trading of goods and services through classifieds, online auctions, or other means not including "traditional" online business-to-consumer models
- **Botnet** – Web pages or compromised web servers running software that is used by hackers to send spam, phishing attacks and denial of service attacks
- **Cartoons, Anime & Comic Books** – Web pages dedicated to animated TV shows and movies or to comic books and graphic novels
- **Child Abuse Images** – Web pages that show the physical or sexual abuse / exploitation of children
- **Command and Control Centers** – Internet servers used to send commands to infected machines called "bots."
- **Compromised** – Web pages that have been compromised by someone other than the site owner, which appear to be legitimate, but house malicious code
- **Gambling** – Web pages which promote gambling, lotteries, casinos and betting agencies involving chance
- **Gaming** – Web pages consisting of computer games, game producers and online gaming
- **Gay, Lesbian or Bisexual** – Web pages that cater to or discuss the gay, lesbian, bisexual or transgender lifestyle
- **Hacking** – Web pages with information or tools specifically intended to assist in online crime such as the unauthorized access to computers, but also pages with tools and information that enables fraud and other online crime
- **Hate Speech** – Web pages that promote extreme right/left wing groups, sexism, racism, religious hate and other discrimination
- **Humor** – Web pages which include comics, jokes and other humorous content
- **Illegal Drugs** – Web pages that promote the use or information of common illegal drugs and the misuse of prescription drugs and compounds
- **Kids Pages** – Web pages specifically intended for young children (under 10) including entertainment, games, and recreational pages built with young children in mind
- **Malware Distribution Point** – Web pages that host viruses, exploits, and other malware
- **Marijuana** – Web pages about the plant or about smoking the marijuana plant. Includes web pages on legalizing marijuana and using marijuana for medicinal purposes, marijuana facts and info pages
- **Miscellaneous** – Web pages that do not clearly fall into any other category
- **Motorized Vehicles** – Web pages which contain information about motorized vehicles including selling, promotion, or discussion. Includes motorized vehicle manufacturers and sites dedicated to the buying and selling of those vehicles
- **Music** – Web Web pages that include internet radio and streaming media, musicians, bands, MP3 and media downloads
- **Nudity** – Web pages that display full or partial nudity with no sexual references or intent
- **Online Ads** – Companies, web pages, and sites responsible for hosting online advertisements including advertising graphics, banners, and pop-up content. Also includes web pages that host source code for dynamically generated ads and pop-ups
- **Pay to Surf** – Web sites that offer cash to users who install their software which displays ads and tracks browsing habits effectively allowing users to be paid while surfing the web
- **Peer to Peer** – Web pages that provide peer-to-peer (P2P) file sharing software
- Phishing/Fraud – Manipulated web pages and emails used for fraudulent purposes, also known as phishing

- **Photo Sharing** – Web pages that host digital photographs or allow users to upload, search, and exchange photos and images online
- **Pornography** – Web pages which contain images or videos depicting sexual acts, sexual arousal, or explicit nude imagery intended to be sexual in nature
- **Profanity** – Web pages that use either frequent profanity or serious profanity
- **R-Rated** – Web pages whose primary purpose and majority of content is child appropriate, but who have regular or irregular sections of the site with sexually themed, non-educational material
- **Redirect** – Web pages that redirect to other pages on other web sites
- **School Cheating** – web pages that contain test answers, pre-written term papers and essays, full math problem solvers that show the work and similar web sites that can be used to cheat on homework and tests
- **Sex Education and Erotic** – Web pages with sexual content or products or services related to sex, but without nudity or other explicit pictures on the page
- **Social Networking** – Social networking web pages and online communities built around communities of people where users "connect" to other users
- **Spam** – Products and web pages promoted through spam techniques
- **Sports** – Web pages dedicated to training and contests involving fighting disciplines and multi-person combat sports such as martial arts, boxing, wrestling, and fencing
- **Spyware** – Web pages containing software that reports information back to a central server such as spyware or keystroke loggers
- **Streaming and Download Video and Music** – Web pages with repositories of music or that provide streaming music or other audio files that may pose a bandwidth risk to companies
- **Television and Movies** – Web pages about television shows and movies including reviews, show times, plot summaries, discussions, teasers, marketing sites, etc.
- **Torrents Repository** – Web pages that host repositories of torrent files, which are the instruction file for allowing a bit torrent client to download large files from peers
- **Unreachable** – Web pages that give an error such as, "Network Timeout", "The server at example.com is taking too long to respond," or "Address Not Found".
- **Violence** – Web pages that promote questionable activities such as violence and militancy
- **Weapons** – Web pages that include guns and weapons when not used in a violent manner

II. Strictly prohibited to download movies, music and apps

III. All internet access will be monitor and manage by the Untangle Firewall and PFSense

IV. Per user quota for accessing the internet per week is **1gb**, ICT Officer can top-up the quota when the reason of excessive that 1GB is reasonable.

V. Accessing social media network and other, will be open during lunch hour and after working hour.
   - Lunch Hour = 12:10pm to 13:40pm
   - After Hours = 16:05pm to 18:00pm

F. Laptop and Desktop Policy

i. Entitlement for the laptop is only for Level 6 and above
ii. From Level 7 and below will entitle for Desktop
iii. Entitlement of Laptop from Level 7 and below is with the approval from the Secretary of MCIC.

G. Server Privilege User

I. Administration
- The user as a right to manage and administrate the system setup, normally the ICT Officer use this user's privilege.

II. Domain User
- The user are restricted to their domain grouping and match to the Divisional level.

III. Guest User
- The user are people that works on temporary, contract and project officers.

H. Sever Shared Drive

I. Non restricted Drive
- Common Shared Drive – will be access by all staff
- BRC Shared Drive – will be access only by the BRC Staff
- BPC Shared Drive – will be access only by the BPC Staff
- Admin Shared Drive – will be access only by the Admin Staff

II. Restricted Drive
- Division and Section Drive – the shared drive will be specific for each individual division and units.

I. ICT Division Right

I. Consulting the ICT Office before purchasing a computer for recommendation
II. Administrative right access to all Computers
III. Has a right to delete any unnecessary Data, Software, Image and movies from computers
IV. Has a right to take and suspense any staff from using MCIC Computer when violate the **ICT Policy C. I - XII**
V. To move any computer within the MCIC for fair distribution of computers
VI. ICT Division own all the computers within Ministry of Commerce, Industry and Cooperatives
VII. ICT Division has a right to collect a computer from retired officer and departed officer to other ministries or organisation.

J. Damage and Lost of ICT Equipment

i. Lost or Damage will be a responsible of the Officer to replace it to the new one, or it will deduct from his/her salary the cost of the replacement.
ii. Unless the police investigation report attaches due to lost from theft
iii. Damage during official matter will be a responsibility of the ICT and BIU Division useless the damage is due to the officer negligence.
iv. Junior Staff Laptop will be lock at the office, by laptop lock which will be provide by the ICT.

ICT Guide Lines

K. New Computer Setup

1. Create the Admin accounts with the ICT Known password
2. Language English US
3. Format date is Australian English
4. National date as Fili or Australia date time, better if there is Kiiribati Time
5. Operating system should be 64 bit and windows 7 or 10
6. Install the Microsoft office 2010 or above
   - Words
   - Excel
   - Access point
   - Power point
7. Install acrobat PDF Software
8. Install PINGIN Messenger
9. Install VNC viewer as the server
10. Install the antivirus (Licensed)
11. Update the andtivirus
12. Configure the antivirus to automatically scan USB, and automatically scan the computer or laptop after starting it……..`0 to 15 delay start time
13. Install the firefox and chrome browser
14. Install the printer's driver if exist
15. Configure the email outlook only in windows 10 to the officer official email of commerce.gov.ki
16. Rename the computer or laptop to officer first letter of his/hers first name follow by surname.
    a. Burenteun Taomati computer= BTAOMATI-PC
    b. Anamari Tengenge laptop = ATENGENGE-LT
17. Create the user account with only users right or permission.

L. Add a New Email User

Non Shuffle Staff

- Business Regulatory Centre
- Business Promotion Centre
- Administration Division
    - All ICT and BIU Officers
    - Legal Officer
    - Drivers
    - Cleaners

First letter of the officer name follow by the surname of the officer for example:

John Doe (Cooperative Officer) = jdoe@commerce.gov.ki

Alias email address for the above officer as follow:

co@commerce.gov.ki

Shuffle Staff

- Administration Division
    - All Admin Officers
    - All Registry Officers
    - All Accounts Officers

Title of the officer as follow:

John Doe (Secretary) = secretary@commerce.gov.ki

Alias email for First letter of the officer name follow by the surname of the officer for example:

John Doe (Secretary) = jdoe@commerce.gov.ki

M. Adding a new Domain User

Adding a new user for the MCIC Domain will be a same procedures for adding a new email user.

First letter of the officer name follow by the surname of the officer for example:

John Doe (Cooperative Officer) = jdoe@commerce.gov.ki

Assign the user with their own drive and common share drive. Joining the new user with their respective Division and Unit.