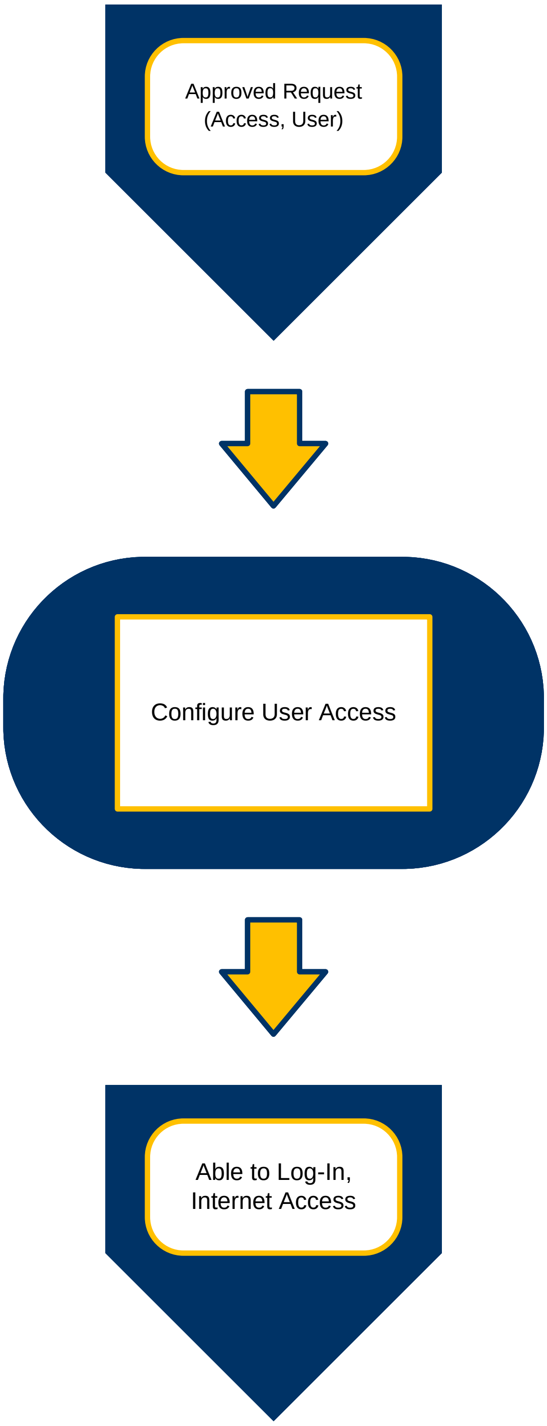
INFORMATION TECHNOLOGY GROUP	INTERNET USAGE GENERAL PROCESS FLOW	Date Created : August 6, 2018 Revision No. : 1 Revision Date : April 1, 2023 Policy No. : ITG-2019-004



Approved Request (Access, User)

Configure User Access

Able to Log-In, Internet Access

1.0. OBJECTIVE

1.1 The purpose of this policy is to enforce the appropriate uses of the Internet by CVMFCC employees.

2.0 SCOPE

2.1 The Internet Usage Policy applies to All internet users (individuals working for CVMFCC) who access the internet through the computing or networking resources. The Company’s internet users are expected to be familiar with and to comply with this policy, and are also required to exercise their good judgement while using internet services.

3.0. DEFINITION OF TERMS

3.1 Email – Send/receive e-mail messages to/from the internet (with or without document attachments)

3.2 Navigation – WWW services as necessary for business purposes, using a (HTTP) browser tool. Full access to the internet; limited access from the specific websites.

3.3 File Transfer Protocol (FTP) – Send data/files and receive in-bound data/files, as necessary for business purposes.

3.4 WWW – World Wide Web (Internet)

3.5 HTTP(S) – Hyper Text Transfer Protocol (Secure)

4.0 POLICY

4.1 INTERNET USAGE

4.1.1 Request and Approval of Internet Access

4.1.1.1 User must fill-up Internet Access Request Form together with Policy awareness acknowledgement form.

4.1.1.2 Signed approval of Immediate Superior and/or Team manager

4.1.1.3 Submit to ITG Team

4.1.2 Internet Usage Do’s and Don’ts

4.1.2.1 Internet access is to be used for business purposes only

4.1.2.2 Capabilities for the standard internet services will be provided to users as needed.

4.1.2.3 Prohibited usage, which employees must not use the network to:

4.1.2.3.1 Download or upload obscene, offensive, illegal or pornographic materials.

4.1.2.3.2 Send confidential information to unauthorized recipients.

4.1.2.3.3 Invade another person’s privacy and sensitive information.

4.1.2.3.4 Download or upload movies, music, games and other that consume significant amount of internet bandwidth.

4.1.2.3.5 Download or upload of unauthorized computer applications.

4.1.2.3.6 Visit potentially dangerous websites that can compromise the safety of our network and computers.

4.1.2.3.7 Access Social Media sites especially for personal use.

4.1.2.3.8 Videos, music, radio and live streaming.

4.1.2.3.9 Perform unauthorized or illegal actions, like hacking, fraud, buying/selling merchandise, raffle ticket, etc.

4.1.2.3.10 Download or upload obscene, offensive, illegal or pornographic materials.

4.1.2.4 Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet “wallets” may do so at their own risk.

4.1.3 Quarterly Review of Network Usage

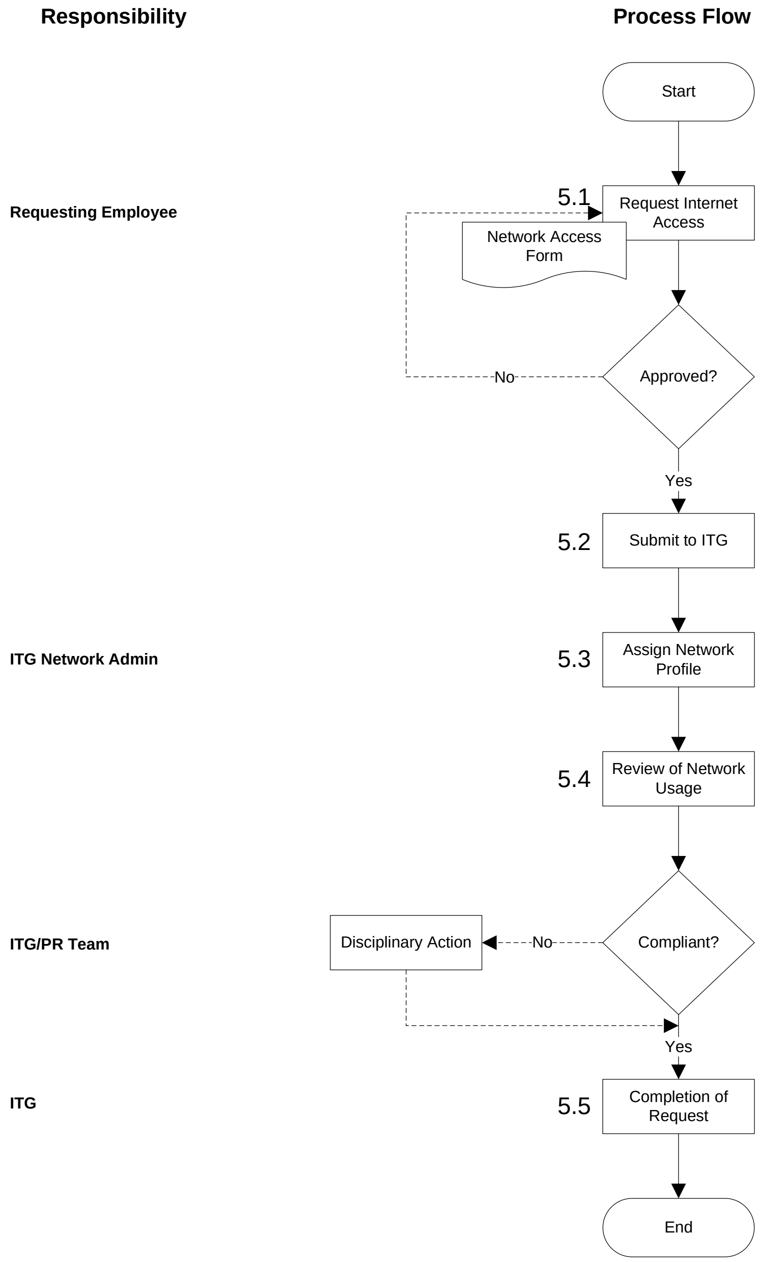
4.1.3.1 Generate report logs from Firewall/Server.

4.1.3.2 Reviewed by ITG Network Administrator.

4.1.4 Non-Compliance

4.1.4.1 An employee found to have violated this policy may be subject to disciplinary action as referred to Employee Handbook Employee Discipline Class B Offense 3

5.0 GUIDELINES



Guidelines

5.1 Request Internet Access

5.1.1 User must fill-up Network Access Request Form which needs to be duly accomplished and approved by immediate superior and/ or team manager.

5.1.2 Rank and file employees network connection will be at Standard connection with restriction to games, music, social media and video streaming, etc. Unless, requested through Network Access Request that will be used for business purposes.

5.2 Submit to ITG

5.2.1 Duly accomplished Network Access Request Form must be submitted to ITG for further processing. Otherwise, request access will be put on hold or not be processed further.

5.3 Assign Network Profile

5.3.1 ITG Network Administrator will assess and assign a network profile for the requesting employee that is categorized depending on the usage or access needed.

5.4 Review of Network Usage

5.4.1 Once network access is already granted and applied. Network Administrator has the rights to randomly checked if the given access profile is used without violating the unnecessary activities mention under clause number 4.1.2.3.

5.4.2 If the requesting employee can completely access the requested network access and is a compliant as well when it comes to usage, request can now be considered as completed. Otherwise, for uncompliant findings, requesting employee may be subject for disciplinary action of PR Team.

5.4.3 After having the requested access, Network Administrator has the right to randomly check its usage in the future or as scheduled under clause number 4.1.3 , and may proceed to disciplinary action request for any uncompliant activity or violation of the Network Usage Policy.

5.5 Completion of Request

5.5.1 Once, aforementioned steps are completed, ITG will now consider this request as fully completed.

6.0 FORMS

6.1 Network Access Request Form – ITG-2018-F-004-A

7.0 AUTHORIZED SIGNATORIES

No.	FORM	SCOPE	SIGNATORIES
7.1	Network Access Request Form	Requested by Approved by Serviced by	Requesting Team Team Head ITG Specialist

8.0 SANCTIONS : Non-compliance on this policy shall be subject to sanction in accordance with the employee code of conduct.

9.0 EFFECTIVITY : This policy will take effect on June 1, 2023

10.0 ACKNOWLEDGEMENT TO COMPLY AND IMPLEMENT

This is to acknowledge that we:

10.1 Reviewed the policies and procedure herein;
10.2 Agree with contents hereof; and
10.3 Commit to strictly implement these policies and procedures.

ELMER M. CATANGAY
Finance and Services
Team Head

MICHAEL B. FRANCISCO
Collection and Recovery
Group Head

DAISY JANE C. CERTEZA
Treasury and ROPOA
Group Head

LEA A. STA. MARIA
Control and Securities
Group Head

CATHERINE PACUAN
Operations Management
Group Head

ROVIELYN P. NATIVIDAD
Data Analytics and Virtual Verification
Team Head