Federal Communications Commission

Information Technology and Privacy Rules of Behavior (ROB)

The FCC provides access to Information Technology (IT) computing resources (hardware, software, and information) to its employees and contractor staff. These resources are provided to facilitate completion of assigned responsibilities, with prior authorization. Policies governing FCC computing resources are further detailed in the FCC Cybersecurity and Privacy Policy. The current version of the policy can be found on the FCC IT Intranet page at: http://intranet.fcc.gov/omd/it/security.php.

All information contained on FCC computing resources is subject to monitoring by authorized FCC personnel at any time. Individual users of the FCC information and systems should not have any expectation of privacy while accessing FCC computers, networks, or e-mail.

Individuals authorized to use FCC computing resources shall be aware that all FCC-owned computer resources assigned, controlled, accessed, and maintained by FCC employees and contractor personnel are subject to periodic test, review, and audit by the FCC.

All individuals who use FCC computing resources must comply with the FCC Cybersecurity & Privacy Policy, relevant IT policies and procedures, and the specific Rules of Behavior listed below. No bureau or office has the authority to relax or modify the requirements set forth herein. Your acknowledgement of these Rules of Behavior constitute agreement; such compliance is required and is a condition prerequisite of your authorization to use FCC computing resources. You understand that non-compliance may constitute misuse of Government property or resources in violation of Federal regulations and FCC policies and may subject you to criminal, civil, disciplinary, or adverse action.

I agree that:

- I will complete mandatory Computer Security Awareness Training before accessing any FCC system, will complete subsequent refresher training as required, and will comply with all conditions and requirements set forth in such training before and while accessing any FCC system or computer resource.
- I will always comply with all copyright and license restrictions on FCC computing resources.

I will only use FCC computing resources for official FCC business, except that limited personal use is permissible so long as it is *de minimis*, does not interfere with performance of official duties, does not impact the security of information and information systems, does not cause degradation of network services, and does not result in any additional cost to the Agency. I acknowledge that limited personal use does NOT allow for any Prohibited Use, as defined below.

- I will not use FCC computing resources to perform any illegal, unethical, or inappropriate activities. Examples of such Prohibited Uses include, but are not limited to:
  - Viewing, downloading, accessing, searching for, transferring, sharing, storing, creating, sending, or providing access to any type of restricted or inappropriate material, messages, or content
  - Gambling or gaming
  - Lobbying Congress or any other federal, state, or local government with respect to any pending or proposed legislation, resolution, appropriation, or measure
  - Engaging in political activity, including campaigning

  - Using, downloading, or distributing illegal copies of copyrighted materials such as software, music, or videos
  - Conducting private or personal for-profit activities
  - Conducting unauthorized not-for-profit activities, such as solicitation for charities, religious, or political causes. Exceptions to this include, for example, the FCC participation in the Combined Federal Campaign
  - Accessing classified information from an unclassified network without a current security clearance and a need to know, even if that information is on the Internet.
- I will abide by applicable federal laws or orders, FCC directives or policies, including, but not limited to, those governing official use of social media, cybersecurity compliance, telework, and remote access.
- I will not access FCC computing resource without utilizing one of the following authorized multi-factor authentication (MFA) methods, in addition to any password and/or PIN required by the relevant system:
  - RSA SecureID (physical or smartphone app)
  - Okta Verify (smartphone app)
  - FCC issued Personal Identity Verification (PIV) card
- I will handle FCC information according to FCC policies and procedures.
  - I request assistance from the Cybersecurity[1] or Privacy[2] team if I have questions regarding the proper handling of FCC information.
- I will log-off or lock devices when unattended as I am responsible for any activity that occurs on my assigned user account.
- I will immediately report any violations or requests by others to violate these Rules of Behavior to the Cybersecurity team.
- I understand that personal credentials (including User IDs and passwords) issued are only for my use, I will not disclose these credentials to anyone at any time for any reason, except as required by the FCC CISO and/or appropriate law enforcement authorities.
  - If I think my credentials are known by another party (someone other than myself) I will change the credentials immediately and create a ticket with the FCC Service Center.
- I understand that ANY document, message, email, or other material sent, received, created, or stored via FCC resources may become an official record, and I have no right to privacy.
- I will not send or post threatening, harassing, intimidating, abusive, or inappropriate material or messages.
- I will not conduct any FCC official business on personal email or forward any non-public data to personal accounts.
- I will not attempt to access any data, systems, or perform any action which is not required in normal execution of my job responsibilities.
  - If I discover I have more access than is required to execute my job responsibilities, then I will immediately report this to the FCC Service Center.
- I will not attempt to bypass any technical or other controls that limit access to computing resources.
  - If additional access is required, I will open a ticket with the FCC Service Center requesting access with proper business justification.
- I will not install any unapproved software on FCC controlled computing resources.
  - If I have questions about whether software is approved, I will create a ticket with the FCC Service Center.
- I will not remove any computing resources from an FCC facility except as required by official FCC business and following all defined policies and procedures.

Virtual Private Network (VPN)

- Personal VPNs are not to be used, prior to connecting to the FCC network.

[1] cybersecurity@fcc.gov

[2] privacy@fcc.gov

Telework

- At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.
- I will physically protect any GFE or personal device I use for teleworking when they are not in use.
- I will protect sensitive data at my alternate workplace. This includes disposing of sensitive information by shredding or other appropriate means.
- I will avoid downloading FCC information on personal devices to ensure all data is contained within the FCC network. This includes downloading FCC attachments outside of FCC OneDrive or SharePoint.
    - If I do download attachments to my personal device, I will move the information to an approved FCC storage location such as, OneDrive, SharePoint, or a shared drive. I will permanently delete the information from my personal device.

Privileged User Access

- I am responsible for all actions taken under my privileged account. I understand that exploitation of my account(s) may have catastrophic effects on all applicable FCC IT resources.
- I will use my Privileged User account only to perform authorized privileged activities.
    - I will use my non-privileged (i.e., general) user account to perform general day-to-day desktop functions (e.g., email, word processing, Internet access, timekeeping).
- I will ensure personally identifiable information (PII) is properly secured and restricted from general access using approved data loss prevention tools and privacy controls as applicable to the environment (e.g., SharePoint, OneDrive, etc.)
- I will not use my privileged account to grant unauthorized privileges to other users to make any unauthorized modifications, access, browse, modify, copy, or delete data/information.
    - I will not access, modify, configure, or use operating systems, cloud environments, software applications or programs except as specifically authorized.
- I will use multifactor authentication (MFA) to perform privileged functions. I will protect the authentication method used from disclosure.
    - If using username/password for a privileged account, I will choose strong, complex passwords in accordance with FCC policy.
    - I will promptly change authentication information whenever compromise is known or suspected.
- I will not make unauthorized copies of security or configuration information (e.g., the etc./password file) for any IT resource.
- I will not attempt to stress, test, circumvent, perform network line monitoring, or conduct keystroke monitoring without authorization.
- I will not connect unauthorized hardware to the FCC network or information system.
- I will not install unauthorized software on FCC information systems (including but not limited to network devices, servers, workstations, appliances, laptops, mobile phones, printers, and copiers).

Privacy Rules of Behavior

I understand that as an FCC employee or contractor it is my responsibility to comply with FCC policies and measures necessary to prevent the unauthorized access, disclosure, modification, or destruction of personally identifiable information (PII).

- I will comply with the following Rules of Behavior when working with PII:
- I will follow FCC privacy policies and procedures, including FCCINST 1113.2, Compliance with Privacy Laws and Guidance, when handling PII whether in paper or electronic form.

- I will seek guidance from the FCC OGC Privacy Team, my supervisor, or Contracting Officer Representative (COR), as appropriate, if I have any questions on how to protect PII.
- I will complete mandatory training provided by the FCC related to privacy.
- I will not exceed my authority to access PII.
- I will not use PII for a purpose other than that which it is authorized.
- I will not disclose PII to unauthorized persons or entities.

Security Incidents and Privacy Reporting

In the case of a security incident or privacy breach, I will immediately report within 1 hour of discovery, any suspected security or privacy incidents, suspicious behavior, and/or unauthorized access to the Network Security Operations Center (NSOC) at NSOC-Monitor@fcc.gov.

Disciplinary Actions

I understand that if I do not comply with the ROB, I may be subject to disciplinary or adverse actions and criminal penalties that may be imposed under federal law. I understand that the FCC may take corrective action against employees and contractors who fail to protect data including, but not limited to:

- Removal of an individual's authority to access FCC information systems or data
- Revocation of an individual's security clearance, if applicable
- Employee discipline, up to and including removal
- Contractor suspension or debarment
- Seeking damages under applicable contract law
- Reimbursement to the government for unauthorized charges
- Criminal prosecution

Moreover, legal actions that may result in civil or criminal penalties may also be initiated by third parties including, but not limited to, the Office of Inspector General, the Department of Justice, and individuals harmed by my action or inaction.

Contact Details

FCC Service Center
Service-Center@fcc.gov
202-418-1200

User Certification

I certify that I have read the above statements, fully understand my responsibilities, and agree to comply. I recognize that any violation of the requirements indicated above may be cause for disciplinary actions, up to and including removal.

Full Name:

Bureau/Office:

Signature:

Date: