Rules of Behavior—Technical Standards RevCom

Access to the RevCom System, and any associated applications, is granted to you based on the following expectations.

1. **Information obtained from RevCom** is to be used for official business only.

2. **Authorized Access:** All requests for access must go through the Office of Sustainability (AU-21) for authorization.

    a. AU-21 will then contact the RevCom Helpdesk to coordinate the granting of the appropriate privileges using standard network security constraints and profiles.

    b. In the event that you no longer require access to RevCom, or you leave the employment of DOE or its authorized contractor organizations, you will notify the RevCom Helpdesk to terminate your user account.

    c. You are to protect any information obtained from RevCom--whether in the form of printed reports or electronic files--against any purposeful or incidental distribution to anyone not authorized access to such data.

3. **Assignment and Limitations of System Privileges:** The privileges provided to you are adequate to perform the normal functions associated with RevCom.

4. **Remote Access:** HS-21 authorizes remote access through the web interface to some functions in the system.

5. **Disposal of IT Resources:** Dispose of IT resources in accordance with current HS-21 policy and direction. At a minimum, erase fixed media prior to transferring the IT resources or designating the resource for excess.

6. **Individual Accountability:** Never share your login credentials, user ID/password, with anyone.

    a. Never leave a workstation unattended when you are logged on.

    b. Workstations unattended for 30 minutes or more must be paused.

    c. Do not log in to more than one workstation/terminal unless you can keep each under constant surveillance.

    d. When access to these IT resources is no longer required, notify HS-21 and make no further attempt to access these resources.

7. **Limits on System Interconnection:** All system changes, regarding interconnections/interfaces with other systems, are under the strict control and approval authority of the CIO and therefore must be coordinated and approved prior to implementation into the production system.

8. **Reporting IT Security Incidents:** Any unauthorized penetration attempt or unauthorized system use, or virus activity will be reported to your supervisor.

Users should also report the security incident to the DOE Headquarters Enterprise Service Center Helpdesk at 301-903-2500.

9. **Restoration of Service**: Restoration of service is in accordance with the MOU between HS-21 and Doxcelerate Corporation along with the RevCom Disaster Recovery Plan.

10. **Software Installation**: Any request for software installation should be coordinated with your local system/network administration office.

    a. Only authorized technicians will be allowed to install software on a DOE workstation.

    b. No personally owned, provided or downloaded software may be installed.

11. **Use of Personally Owned Information Systems**: Personally owned or provided hardware and/or information systems may not be used to conduct official business.

12. **Password for RevCom access:** You agree the following guidelines. The password:

    c. contains between 8 and 20 non-blank characters;

    d. contains at least one number;

    e. must start and end with a letter;

    f. must contain at least one special character and can only be either # or $;

    g. does not contain the user ID;

    h. does not include the user's own or, to the best of his/her knowledge, close friends or relatives names, employee serial number, Social Security number, birth date, phone number, or any information about him/her that the user believes could be readily learned or guessed;

    i. does not, to the best of the user's knowledge, include common words that would be in an English dictionary, or from another language with which the user is familiar;

    j. does not, to the best of the user's knowledge, employ commonly used proper names, including the name of any fictional character or place;

    k. does not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx";

    l. is different than the passwords employed by the user on his/her classified systems.

13. **Password Protection:** You agree to protect your password in the following manner:

    a. You will not share Passwords except in emergency circumstances or when there is an overriding operational necessity

b. You will not leave clear-text Passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the Password

c. You will not enable applications to retain Passwords for subsequent reuse.

d. Passwords must be changed:

- at least every 6 months
- immediately after sharing
- as soon as possible, but within 1 business day after a Password has been compromised, or after one suspects that a Password has been compromised
- on direction from management.

14. **Protection of Personally Identifiable Information (PII)**

- Any remote access to the DOE network to access data in this system must be made through a VPN using two-factor authentication if the data you are accessing is other than your own. Two-factor authentication is where one of the factors is provided by a device separate from the computer gaining access
- All PII media other than your own (i.e., hard copy reports or information loaded to a CD, thumb drive, or any other removable electronic media) that is transported (see definition below) will be encrypted using FIPS 140-2 or greater compliant software.
- Any and all files that contain PII that are sent via e-mail will be encrypted using Entrust.
- PII that is stored on Laptops or removable media or at a remote location must be deleted within 90 days or when no longer needed for official business purposes.

Consequences of Behavior Inconsistent with the Rules: Failure to adhere to these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

I have carefully read and fully understand the explanation of responsibilities and the applicable penalties for failure to abide by the above Rules of Behavior in regards to RevCom.

_____ _____

Signature Printed Name

_____

Date