Fire Engine RED

REMOTE SECURITY POLICY

This Remote Security Policy describes how we do things at Fire Engine RED. While we cannot guarantee that it meets your legal requirements, you are free to adapt/reuse any of the material for your fully remote (or not) company.

This Remote Security Policy should be viewed within the context of being a 100% remote company with no central office location. With that in mind, the policy applies to all employees and contractors, whether they're working in a home office or at a coffee shop, shared workspace, hotel, conference, client's campus, etc.

Your Equipment

Your computer is company property. You should keep it clean, safe, and out of the reach of children, pets, or anyone who might tamper with it.

YOU'RE ALSO REQUIRED TO:

- Password-protect your computer.
- Enable your firewall, and leave it on. (By default, it should be on the "deny all" setting; you should only allow access to trusted applications.)
    - **Mac:** Go to System Preferences > Security & Privacy > Firewall > Turn On Firewall Make sure the box next to "Block all incoming connections" is checked.
    - **Windows**: Firewall is enabled by default.
    - **Linux:** If you're running Linux, you know what to do.
- Install and regularly update your antivirus software (on Macs and PCs; yes, Macs are susceptible to malware and trojans, too). Free programs include:
    - AVG (http://free.avg.com/us-en/free-downloads)
    - Avast (http://www.avast.com/en-us/download-software)
- Set your screensaver to lock after 10-20 minutes of inactivity. (If you're working in a public place, you should lock your screen any time you walk away from your computer.)
- Enable your firewall, and leave it on. (By default, it should be on the "deny all" setting; you should only allow access to trusted applications.)
    - **Mac**
        - Hard drive – File Vault (https://support.apple.com/en-us/HT204837)
        - Backup drive – Time Machine (https://support.apple.com/en-us/HT201250)
    - **Windows**
        - Hard drive: (https://support.microsoft.com/en-ca/help/4028713/windows-10-turn-on-device-encryption)
    - Encrypt specific files and folders that contain sensitive data (this applies specifically to members of our Client Care, Data Services, Finance, P3, and Sales teams).
        - Veracrypt (https://www.veracrypt.fr/en/Home.html)

- Keep your operating system up to date – install major releases and patches immediately

- Back up your computer to the cloud or to an external hard drive. You should have the ability to quickly recover your work.

INFORMATION SECURITY

You're required to protect any and all of the company's proprietary and confidential (internal or client) information.

With this in mind, you must:

- Use the company VPN when working from somewhere other than your home office (e.g. coffee shop, airport, hotel, conference, shared workspace, etc.).

- Use our secure FTP site to store and share business-sensitive documents (contracts) and personally identifiable information (client/student data), using our secure FTP site.

- Use strong, unique passwords for each of your accounts and tools. We recommend that you:
    - Install password management software.
    - Use complex passwords (a minimum of six characters and a combination of alphanumeric, upper and lowercase, and special characters) for access to all company-wide and departmental tools, as well as for your computer. Never use a common or simple password (e.g., 123456789, Password, qwerty, 111111, etc.).
    - Change your passwords:
        - Every three months.
        - After using a public Wi-Fi network.
        - If you think they have been compromised.

- Keep your usernames and passwords secure – NEVER write them down or provide them to anyone via email or text.

- View confidential information only on secure devices.

- Use 2FA (Two-Factor Authentication) when available.

- Keep your company files and other materials separate from your personal files and clearly marked as property of Fire Engine RED.

- Avoid opening (or acting on) email that appears suspicious or asks for login information or something out of the ordinary.
- Avoid clicking suspicious links. If you suspect a link may be fraudulent, mouse-over it to view the actual URL before clicking.
- Refrain from downloading suspicious, unauthorized, or illegal software.

A note from the *Fully Remote* team:

Thank you for reading *Fully Remote* and for downloading one of our valuable resources!