SAN DIEGO STATE UNIVERSITY

IT Security Guidance for Remote Access

University employees have the ability, in many cases, to access the University's information systems from computing devices and locations other than their regular workspace and outside of the University's network.

Remote access puts systems at higher risk for attacks and unauthorized access because if the system is accessible to employees/faculty and students from outside of the University's network, it is also accessible to hackers and criminals. This translates to an increased likelihood that University information could be impacted from a confidentiality, integrity, or availability perspective.

Additional precautions should be taken by employees when working remotely.

1. Security Measures

- If possible, use an SDSU managed device.
- If you access University information systems remotely from a non-SDSU State device, the IT Security Office encourages you to consider the following:
  - **Use anti-virus/anti-malware software** and configure it to automatically update. This also includes your mobile device.
  - **Configure your operating system and applications to automatically apply updates** (e.g., Microsoft updates or Mac updates.)
  - **Don't use the "remember my password"** feature when accessing University information on a shared device.

In addition, follow these best practices:

- **Don't share or re-use passwords** used to access University information and systems.
- **If possible Do Not Share Your Device**: If you are working from home and are forced to use your personal device, make sure you are the only one using your device. SDSU data cannot be shared with family members. Allowing others to use a device that is being used to access SDSU data violates SDSU policy by potentially sharing it with persons that have no right to see SDSU data, including your spouse.

- **Patch All of Your Software**: Updates to device software and other applications can sometimes take a long time, but they really are important. Updates often include patches for security vulnerabilities that have been uncovered. Patch your home computer.
- **Protect passwords used to access University information**, and consider using a password manager like LastPass.
- **Do not store files locally**. Access all files directly in the file share or on Google Drive.
- **Use VPN software to protect your communications** when you connect to public Wi-Fi networks. You should not consider your online activity to be private when using public Wi-Fi networks.
- **Use Eduroam to connect to Wi-Fi if visiting participating campuses** and institutions worldwide. Connect using your SDSU credentials.
- **Report the incident** to the appropriate delegated authority If a device containing University information is lost, stolen, or compromised
- **Email Security** – Do not send Protected Level 1 information (confidential data) in an email message. Be on alert for phishing scams; look out for phishing emails and sites. Phishing emails, as well as voicemails (vishing) and text messages (smishing), are used by cybercriminals to steal your and SDSU's information. Forward any suspicious emails to fraud@sdsu.edu.
- **Never Leave Your Devices or Laptop in the Car.** Never leave your work computers or devices in a vehicle. It is a best practice to keep work laptops and devices on your person at all times. The trunk of your car is not any safer. There may be criminals watching the parking lot from afar, waiting for their next victim. Putting valuables in the trunk may make life a little bit easier in the short-term - but why take that chance?

2. VPN

If you require access to certain shared drives or servers behind the firewall, you will need to make sure VPN software is installed and tested before you leave the office. Follow the install guide here or talk with your IT support staff.