STAFF

Virtual Private Network (VPN) & Remote Access Policy

1) Scope -
The purpose of this policy is to define the guidelines for the use of VPN and/or Remote Access (i.e. SFTP, SSH, etc.) to connect to the School of Visual Arts' (SVA) network. This policy applies to all Student workers, Full or Part Time Staff, Temporaries, and other workers, including all personnel affiliated with third parties, utilizing VPN, SFTP, SSH, etc. as a method to access the SVA network.

2) Policy -
Approved SVA employees, student workers, etc., may utilize the benefits of VPN, SFTP, SSH, etc. which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying any associated fees. While the below sub-policies are explicitly called out, they are not exclusive. Any action that violates the generally accepted standard of conduct among business and corporations, or our Electronic Code of Conduct, may be subject to legal action at the discretion of SVA.

Additionally,

A) It is the responsibility of employees and other authorized users with VPN, SFTP, SSH, etc. privileges to ensure that unauthorized users are not allowed access to SVA's networks by protecting and securing their equipment.

B) You may not connect to another network, other than the network you are on when initiating the connection, while connected using the VPN, SFTP, SSH, etc. connection.

C) All computers (smart phones, tablets, etc. are also considered computers) connected to SVA networks via VPN, SFTP, SSH or any other technology must use current antivirus and firewall software – this includes Apple computers which are widely (and incorrectly) assumed to be immune to such a need. If no such software is available to the user at no cost, it is the user's responsibility to purchase, install, and maintain this software.

D) VPN, SFTP, SSH, etc. users will be automatically disconnected from SVA's network after a predetermined period of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes may not to be used to keep the connection open.

E) Only VPN clients approved by the Administrative & Network Services department may be used. Currently, this is limited to the Cisco AnyConnect VPN client.

F) By using VPN, SFTP, SSH, etc. technology on/with non-SVA-owned equipment, users acknowledge that their machines are a de facto extension of SVA's network, and as such, are subject to the same rules and regulations that apply to SVA-owned equipment as set forth in the SVA Electronic Communications Code of Conduct, for the duration of the VPN or remote access connection. A copy of the ECCC may be obtained from the Office of Human Resources.

G) SVA provides only minimal technical services to authorized users attempting to establish a VPN, SFTP, SSH, etc. connection, such as confirming whether your hardware and/or software is compatible with our network, or troubleshooting connectivity via VPN, SFTP, SSH, etc. Users are responsible for their own technical support beyond successful connectivity.

3) Enforcement -
Any SVA employee (Student Worker, Full or Part Time Staff, etc.) found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Furthermore, any non-SVA employee found to have violated this policy may have his or her relationship with SVA, terminated, and/or may no longer be eligible to utilize the SVA VPN, SFTP, SSH, etc. connection. In all cases, SVA retains the right to also take legal action if applicable. If there are any questions about this policy or any element thereof, please direct them to the IT Services Help Desk at 212.592.2400 or helpdesk@sva.edu.

Please note: No account will be created unless ALL info is obtained, and ALL signatures obtained

_____ End User Needing Remote Access (**Print**)	_____ End User's Supervisor's Name (**Print**)
_____ End User Needing Remote Access (**Sign**)	_____ End User's Supervisor's Name (**Sign**)
_____ End User's Department	_____ Date of Supervisor Approval
_____ Device Being Used For Access (Apple PC, Windows PC, iPad, etc.)	_____ Director of IT/CIO Approval & Date