# Administrative Access for Endpoints and Servers

University computer administrator access standard approvals

## Requester Details

Requested By: Jason Krisch

Primary Contact Phone: 5405262220

Primary Email: jkrisch@vt.edu

Department: Fralin Biomedical Res. Institute

*Review the following training materials, security standards, and FAQs

Please review the following links below:

PageUp Training

Minimum Security Standard

University Computer Administrator Access Standard

Please review the following explanations for the choices below:

**A:** I certify that I have taken the recommended training listed above and understand how to secure my machine. I also certify that I understand Minimum Security Standards and agree to abide by the University Computer Administrator Access Standard.

**B:** I certify that I have the requisite job-based experience and knowledge to secure my machine. I do not need to take the training above. I also certify that I understand Minimum Security Standards and agree to abide by the University Computer Administrator Access Standard.

**C:** I certify that my role and job description require me to have administrative rights on multiple machines in my department and I certify that I have the requisite job-based experience and knowledge to secure the machines. I also certify that I understand Minimum Security Standards and agree to abide by the University Computer Administrator Access Standard. This choice is intended for IT support professionals who support end points and servers for their department. This option will allow one to input their department code for blanket approval.

After reviewing these materials, please select one of the multiple choice options below:

- (●) A: I certify that I have taken the recommended training listed above
- ( ) B: I certify that I have the requisite job-based experience
- ( ) C: I certify that I am a departmental IT Support person

*Please select your departmental IT technical contact for review

Please select the member from your local IT unit responsible for granting administrative access to machines. The individual selected here will be sent an approval record for initial review. Please partner with your local IT unit before submitting this form if you're unsure who should be reviewing your request. For best results, search via PID.

Jason Krisch

*Please select your department head or authorized approver for approval

The individual selected here will be sent an approval record for review. Please enter the department head, manager, or authorized approver responsible for approving administrative access requests to your machines. Please partner with your local IT unit and manager before submitting this form if you're unsure who should be reviewing your request. For best results, search via PID.

Jason Krisch

*Please provide your business use case for this request

[STATE YOUR BUSINESS CASE HERE]

* Select machine you require administrative access to

- (•) End point: low-risk data
- ( ) End point: moderate-risk data
- ( ) End point: high-risk data
- ( ) Server: low-risk data
- ( ) Server: moderate-risk data
- ( ) Server: high-risk data

Details

Low-Risk Data includes public information or data that, if disclosed, would not cause any financial, reputational or safety concerns to the university. Examples include job postings, campus maps, non-private directory information, public research data and public policies and procedures.

* List the hostname(s) of the system(s) for which you will have admin rights access.

Please list hostnames as comma separated values. Alternatively, if multiple machines all share the same data risk and attributes below, a csv file can be uploaded using the 'Add attachments' icon at the bottom of this form.

[ENTER THE VT000XXXX ASSET TAG OF YOUR DEVICE HERE]

List VT asset tag numbers

Please list asset tags as comma separated values

[ENTER THE VT000XXXX ASSET TAG OF YOUR DEVICE HERE]

* Systems for which I have Admin Rights will be patched within 30 days of the patch being published.

- ( ) I will ensure the patching is done myself
- (•) My department is responsible for timely patching

* Briefly describe the patching process

Patches are pushed automatically to FBRI assets via IT management software. For any unsupported devices, patch management is configured to automatically install patches on release.

* Anti-malware and antivirus protections are installed and scheduled to run full scans every week.

- ( ) I confirm that these protections are in place and scan weekly.
- (•) My department is responsible for these protections

* List the name of the antivirus/anti-malware software used

Symantec Enpoint Protection

* Backups of local user data are made weekly

- ( ) I have implemented regular backups of user data
- (•) My department is responsible for a consistent backup process

* Briefly describe the backup process and software used

FBRI IT encourages all users to store data on the FBRI network or in the cloud. FBRI does not ensure protection of data stored locally.

* System(s) are registered with the the departmental inventory system

- ( ) I have registered the system with the departmental inventory
- (•) My department is responsible for departmental inventory

* A host-based firewall has been properly configured in default-deny mode and permits only necessary services

- ( ) I verify the firewall has been configured
- (•) My department is responsible for firewall configurations

Feedback Help

* At the end of the equipment's functional life, it will be disposed through Surplus Property

- ( ) I will dispose of system through Surplus when end of life is reached
- (•) My department will coordinate with surplus to dispose of retired equipment

*No anonymous system access is allowed. Passwords with age, length and complexity requirements are set and meet VA Tech requirements. A 15-minute inactivity screen-lock is in place.

- ○ I have followed the above requirements to meet Virginia Tech guidelines
- ◉ My department has followed the above guidelines to meet Virginia Tech guidelines

*BigFix or equivalent patch management service has been installed and is actively managed

Select "My department does not use a patch management service" if you do not use Bigfix or an equivalent service and will work directly with your IT Staff to ensure security patches are applied as required by the Minimum Security Standard.

- ○ I have installed and manage BigFix (or equivalent service) on my systems
- ◉ My department uses BigFix (or equivalent service) to maintain system patching
- ○ My department does not use a patch management service

*List the patch management service in use.

Equivalent services include ansible, jamf, intune etc.

ConnectWise Automate, Anisble

Additional comments

Add attachments

Add to Cart

Add to Wish List

**Delivery Time:** 8 Days

Submit

Phone (24/7) : (540) 231-4357

Virginia Tech Home

Division of Information Technology Home



About us

Privacy

Acceptable Use