Administrative Rights

1. **Why is it important that administrative rights be limited?**

   Logging in to a computer using access credentials that allow "administrative rights" allow software to be installed on the device without further action. This allows malicious software to self-install if a user who has signed on with administrative rights clicks on a phishing or other link that brings in the unwanted code. The software can then monitor the user's key strokes to steal access credentials to University systems, alter data on the computer, export data from the device, etc. Once installed on a computer with access to the Yale network, some malicious software will also propagate throughout the network and hence one user who has inadvertently downloaded the software can threaten all computers on the Yale network. A request for an exception can be made to the Chief Information Security Officer.

2. **I need to manage the software on my device and hence need administrative rights. Is there a way to be both compliant and to allow me to manage the software in accordance with my work needs?**

   Yes. An exception can be granted to allow a second set of credentials that must be entered prior to adding new applications to the device. Like encryption exceptions, granting administrative rights poses a risk to the University and will only be granted where necessary for University business purposes. A request for this exception can be made to the Chief Information Security Officer.