Lab Manager Local Administrative Rights Request

In order to reduce the likelihood of malicious software compromising Institute IT systems, users do not normally have local administrative rights on their workstations. If you manage a lab and require local administrative rights please complete this application form, sign it to confirm that you have read and accept the conditions and then forward to your manager for approval.

WARNING: Logging in to a Institute PC with admin rights always poses a level of security risk. Users should take extreme care when web browsing, particularly when downloading software or opening attachments from unknown or untrusted sources.

To be completed by the applicant	
Name:	Department:
Tel No:	Manager:

Please explain why you require local administrative rights and list the locations you will be managing:

IMPORTANT – PLEASE READ BEFORE SIGNING

For all computers that you have administrative rights to control:

1. You are responsible for adhering to all RIT and NTID security standards and policies.
2. All software required by RIT and NTID must be kept installed, updated and functioning.
3. The local admonistrator password will not be changed or the computer modified to prevent an NTID adminstrator from gaining access to the system, including locking files or directories from access by TIS.

4 The installation of unauthorized and unlicensed applications is not allowed.

5 You must conform to the End User License Agreement associated with any software you add. The EULA is a legal contract between the manufacturer and/or the author and the end user of an application. The EULA details how the software can and cannot be used and any restrictions that the manufacturer.

6 You will ensure that all reasonable steps are taken to keep your workstation secure and free from viruses, trojans etc.

7 You will be solely responsible for backup of all files, data, applications or any other data stored on the workstation.

8 It shall be your responsibility to ensure that adequate steps are taken to protect workstation data from loss, theft or damage.

9. In addition, the user understands that any modifications made to the computer that disrupt the usability of the system or software will not be the responsibility of the NTID Department of Technology and Information Services to troubleshoot or repair, and in the event of system instability or unusability, the NTID Department of Technology and Information Services will return the computer to a fresh image state. The user will be responsible for restoring data that was stored locally on the computer, as well as any additional software that the user installed.
10. If the workstation needs to be rebuilt, TIS will install a standard base image. TIS will not reinstall any applications or reconfigure the machine to its previous working state.
11. The Director of Information Security and Technology Services may rescind your administrative rights if these terms are not complied with.
12. TIS reserves the right to amend the conditions of this service as appropriate

Applicant:
I apply for Local Administrative Rights having read, understood and agreed to the above:

______________ (Date) _________________________ **(Please Print)** _________________________ **(Sign)**

To be completed by Head of Department:
I request granting of Local Administrative Rights to the above named member of staff on the basis outlined above:

______________ (Date) _________________________ **(Please Print)** _________________________ **(Sign)**

To be completed by VP/Dean or Designee:
I approve granting of Local Administrative Rights to the above named member of staff on the basis outlined above:

______________ (Date) _________________________ **(Please Print)** _________________________ **(Sign)**