

Full Disk Encryption Exception Form

Process:

- 1) Fill out the information in the Laptop Information section.
- 2) End user signs and dates the form agreeing the terms listed below.
- 3) IT Director of the unit that owns the laptop signs and dates the form agreeing to the terms listed below.
- 4) A copy of this form should be forwarded to ITS – Information Security in either of the methods below:
 - a. Campus Mail : “Information Security – Machinery Hall”
 - b. E-mail: Scan the signed document and send to ITSecurity@listserv.syr.edu

Laptop Information

Make	
Model	
Serial Number	

Terms:

ITS Information Security grants an exception to the **Laptop Full Disk Encryption Standard** for the laptop described above with the understanding that the undersigned end user and unit IT Director accept the responsibility to perform due diligence to ensure that no SU confidential or enterprise data as described in the **Syracuse University Information Security Standard** (<http://its.syr.edu/security/standards/ITSecurity-standard.pdf>) is stored on the laptop’s hard drive. Failure to do so could result in significant financial and reputational losses to the University if the unencrypted laptop is lost or stolen.

End User Name _____	IT Director Name _____
Signature _____	Signature _____
Date _____	Date _____
Unit _____	Unit _____

Return copy of completed form to Information Security as described above.