Laptop Security Policy

1.0 Purpose
The purpose of this policy is to provide guidance for laptop security for Fuqua laptops in order to ensure the security of information on the laptop and information the laptop may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA guidelines are met.

2.0 Scope
This policy applies to all Fuqua faculty, employees, contractors, workforce members, vendors and agents with a Fuqua-owned or personal-laptop connected to the Fuqua network.

3.0 Policy
Appropriate measures must be taken when using laptops to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users in order to protect Fuqua's reputation and intellectual assets. Appropriate measures must also be taken to reduce the likelihood of physical loss or damage to laptops in order to protect Fuqua's capital assets.

3.1 Workforce members using laptops shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.
3.2 Fuqua will implement physical and technical safeguards for all laptops that access electronic protected health information to restrict access to authorized users.
3.3 Appropriate measures include:

- Restricting physical access to laptops to only authorized personnel.
- Ensuring laptops are not left unattended in public places on or off Fuqua/Duke property.
- Securing laptops (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that laptops that were left unsecured will be protected.
- Complying with all applicable password policies and procedures.
- A software firewall (such as Windows Firewall) should be turned on and configured for the minimal access necessary to perform normal work.
- All operating system and application security related hotfixes, service packs and patches should be applied as early as possible after they have been made available.
- Antivirus definitions should be kept up to date.
- Laptops are to be used for authorized business purposes only.
- Never installing unauthorized software on laptops.
- All sensitive information, including protected health information (PHI) should be stored on network servers.
- Keeping food and drink away from laptops in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Mobile Device Encryption policy.
- Complying with the Anti-Virus policy.
- Ensuring that view screen/monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- When left at Fuqua, ensuring laptops are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
- Ensuring, when possible, that all laptops use a surge protector (not just a power strip).
- If wireless network access is used, ensure access is secure by following the Wireless Communication policy.
- If remote access is used to connect to the Fuqua network, ensure the Remote Access policy is followed.
- Ensuring laptops are transported and stored in a padded, protective case, bag, backpack, or other similar luggage. Locks should be employed whenever possible.

- When transported by car, laptops should be stowed in the trunk or some other area where it will not be easily seen or attract attention.
- When traveling by air or train, the laptop should never become checked baggage and should always be kept as carry-on luggage.
- During hotel stays, laptops should not be left unsecured in the room. If the user cannot take the laptop with them when leaving the hotel, it should be secured with a cable lock or left in the hotel safe.
- If network connectivity is required during hotel stays, the user should opt for a wired connection if one is available.
- When used away from Fuqua/Duke facilities, wireless and Bluetooth should be turned off whenever possible to reduce the likelihood of unauthorized access.
- Public Wi-Fi hotspots should be avoided if at all possible. Great caution should be used when connecting to non-Fuqua/Duke operated networks.
- Lost or stolen laptops should be reported to the Duke IT Security Office as soon as possible. The Fuqua Help Desk should also be notified.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Laptops include: laptops, Smartphones, PDAs, computer based medical equipment containing or accessing patient information and authorized home laptops accessing the Fuqua network.

Workforce members include: faculty, employees, volunteers, trainees, and other persons under the direct control of Fuqua

6.0 Revision History

Date	Who made the revision	Change made
2012-02-03	Fuqua Infrastructure	Initial issue

This document was adapted from a draft created by the SANS Institute and is used by permission of the SANS Institute.