

# **A&F ADMIN. SYSTEMS LAPTOP COMPUTER SECURITY POLICY AND PROCEDURES**

## **Purpose and Scope**

This document describes the *Policy and Procedures* that must be followed by all ADMINISTRATION & FINANCE workforce members who use an A&F ADMIN. SYSTEMS-issued laptop computer. Failure to comply with the requirements of this document, any applicable data protection policies and procedures, the University Acceptable Use Policy [http://www.oit.umass.edu/policies/acceptable\\_use/guidelines.html](http://www.oit.umass.edu/policies/acceptable_use/guidelines.html), or any applicable Commonwealth information security policies, procedures, or standards, could result in the loss of laptop privileges.

## **General Requirements**

Each employee issued a laptop is responsible for the security of that laptop, and also for the information stored on it, regardless of whether the laptop is used in the office, at a place of residence, or in any other location such as a hotel, conference room, car or airport.

Upon allocation of a laptop, all users must read the *A&F ADMIN. SYSTEMS Laptop Computer Security Policy and Procedures*. All users will also be required to sign a laptop issuance agreement stating that they agree to comply with the *Policy and Procedures*.

## **Limited Access**

The laptop is for your use in the performance of your work. Do not share your laptop with anyone including other workforce members, family or friends.

## **No Personal or Commercial Use**

The laptop may only be used for activities falling within the scope of your employment with A&F ADMIN. SYSTEMS. You may not use the laptop for personal or commercial use.

## **Prohibition on Installing Software**

Users may not install third-party software, or otherwise alter the configuration of the laptop, unless expressly permitted by A&F ADMIN. SYSTEMS. Any software not installed or explicitly authorized by A&F ADMIN. SYSTEMS is subject to deletion without notice. This includes screen savers, games, software downloaded from the Internet, software brought from home, and software provided by other state agencies.

## **Passwords**

- Do not share or disclose your password with anyone.
- Do not write down your password and store it with your laptop and do not store your password on the laptop hard drive.

- Do not allow web browsers or applications to store passwords and login information as these features are easily compromised by hackers, and your IDs and passwords could be stolen.

### **Data Back-Up**

Data stored on the laptop's hard drive (C drive) can be lost as it is not automatically backed-up. To ensure that your data is not lost, all workforce members issued laptops are responsible for regularly backing-up their data.

- When working remotely, log into <https://umaaffp.adminfin.ads.umass.edu/> on a regular basis and back-up data to network drives.

### **Sensitive Data**

- If sensitive information is stored on the laptop, you must ensure that it is encrypted in a secure file or volume when not in use. Contact A&F ADMIN. SYSTEMS if you need encryption software.
- Do not copy sensitive data to non-secure, non-encrypted portable media such as usb, cd, dvd or floppy disks. Instead, move data to properly secured folder on <https://umaaffp.adminfin.ads.umass.edu/>.
- All uses and disclosures of sensitive information must be in accordance with University Sensitive Data Guidelines [http://www.oit.umass.edu/security/compliance/securing\\_data.html](http://www.oit.umass.edu/security/compliance/securing_data.html).

### **Security at Agency Property**

- While working on agency property, never leave the laptop unattended for any extended time unless it is locked in a cabinet or office.
- Always log off your laptop, or press Ctrl+Alt+Delete and Select "Lock Workstation," when you walk away from it even briefly.
- Do not modify the settings for the automatic screensaver which logs you off the system after 10 minutes.

### **Security When Traveling**

- When traveling, keep the laptop close to you whenever possible.
- Always log off your laptop, or press Ctrl+Alt+Delete and Select "Lock Workstation," when you walk away from it even briefly.
- Always log off your computer and put it and all peripherals in an unobvious carrying case before transporting it between locations.
- Never leave the laptop unattended in public areas such as restaurants, airport lounges, hotels and conference centers.
- Avoid leaving your laptop unattended in an automobile even if the vehicle is locked. If you must do so temporarily, be sure that you are parked in a reasonably secure location such as a parking garage, and the laptop is not in plain sight.
  - For example, you should not leave a laptop stored in a laptop bag in the backseat of your vehicle. This would be in plain sight and visible by passerby. A better solution would be to place it in a locked trunk.

## **Security Incidents**

You must report any security incidents involving your laptop. This will enable A&F ADMIN. SYSTEMS to investigate, and take steps to mitigate the risk to any confidential data maintained on the laptop.

### **Incidents on University Property**

If your laptop was lost, stolen or vandalized while being used on University property, such as your primary office, contact the A&F Admin. Systems as soon as possible. Next, contact your Supervisor who will help coordinate the investigation of the security incident according to agency procedures. You will be required to cooperate with any further investigation.

### **Incidents on Non-Agency Property**

If your laptop was lost, stolen or vandalized from your car or home, or when you were at any other non-agency property, you must immediately file a police report with local police authorities, and must cooperate in any investigation conducted relating to the loss, theft or damage. Be sure to get a copy of the police report which you will need to provide to your supervisor. Upon return to work, contact the A&F Admin. Systems, and then your supervisor. You will be required to cooperate with any further investigation.

DRAFT



# A&F ADMIN. SYSTEMS Laptop Computer Security Issuance Agreement

Upon request, a laptop may be issued to an A&F employee who agrees to abide by the policy and procedures set forth below.

## Policy

Each A&F employee who is being issued a laptop must:

1. Read the A&F ADMIN. SYSTEMS Laptop Computer Security Policy and Procedures; and
2. Sign a Laptop Issuance Agreement stating that they agree to comply with the Policy and Procedures.

I have read the A&F ADMIN. SYSTEMS Laptop Computer Security Policy And Procedures and agree to use the laptop listed below in compliance with such Policy And Procedures, any applicable agency privacy and acceptable use policies and procedures, and any applicable University information security policies, procedures, or standards. This agreement will last until I return the laptop and receive a signed return receipt from my A&F Admin. Systems.

<b>Computer Name:</b>			
<b>Employee's Signature:</b>		<b>Date:</b>	
<b>Issuer's Signature:</b>		<b>Date:</b>	

## Return Receipt

<b>Serial Number:</b>		<b>Date Returned:</b>	
<b>Received By:</b>			
<b>AC adapter:</b> <input type="checkbox"/>	<b>Ethernet Cable:</b> <input type="checkbox"/>	<b>Case:</b> <input type="checkbox"/>	<b>Mouse:</b> <input type="checkbox"/> <b>Lock:</b> <input type="checkbox"/>