

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.05 Computer Security Incidents**  | **Revised: May 20, 2021** |

1. GOVERNING REGULATIONS

This procedure is governed by the following policies and regulations:

1.1 System Regulation [29.01.03](http://policies.tamus.edu/29-01-03.pdf) Information Security

1.2 Administrative Procedure [01.04](http://tfsfinance.tamu.edu/modules/finance/admin/admin_procedures/0104%20Fraud%20Prevention%20Program.docx) Fraud Prevention Program

1.3 Administrative Procedure [30.02](http://tfsfinance.tamu.edu/modules/finance/admin/admin_procedures/3002%20Equipment%20Management.docx) Equipment Management

1.4 Administrative Procedure [50.03](https://tfsfinance.tamu.edu/modules/finance/admin/admin_procedures/5003%20General%20Computing.docx) General Computing

1.5 Administrative Procedure [50.06](https://tfsfinance.tamu.edu/modules/finance/admin/admin_procedures/5006%20Response%20Plan%20for%20Data%20Security%20Breach.docx) Response Plan for Cybersecurity Incidents

1.6 Texas Administrative Code (TAC), Title 1, Part 10, [Chapter 202](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), Information Security Standards

2. GENERAL

Computer security incidents include, but are not limited to, the following:

2.1 malicious code detection (other than virus, spyware, malware),

2.2 unauthorized use of user accounts and computer systems,

2.3 theft of computer equipment or electronic information,

2.4 disruption or denial of service that cause substantial loss of time or money to Texas A&M Forest Service (TFS),

2.5 any unlawful activity with the use of Internet, intranet and email,

2.6 any fraudulent activity involving information resources,

2.7 misuse of privileges,

2.8 unauthorized acquisition, loss or theft of personally identifiable information,

2.9 any activity that violates Administrative Procedure 50.03 General Computing,

2.10 ransomware or encryption attacks.

3. PURPOSE

3.1 This procedure describes and establishes the requirement for dealing with computer security incidents.

3.2 This procedure applies to all designated departments and individuals with authorized access to TFS information resources.

4. REPORTING COMPUTER SECURITY INCIDENTS

 The following reporting procedures shall be followed whenever a computer security incident is suspected.

4.1 Incidents involving fraud, waste or abuse of information resources will be reported in accordance with Administrative Procedure 01.04 Fraud Prevention Program.

4.2 Incidents of any unlawful activity will be reported to the Associate Director for Finance and Administration.

4.3 Incidents of computer theft will be handled in accordance with the Missing, Stolen or Vandalized Equipment section of Administrative Procedure 30.02 Equipment Management. In addition, the IR Department must be notified of a computer theft within one business day.

4.4 Incidents involving personally identifiable information or ransomware attacks will be reported to the IR Department in accordance with Administrative Procedure 50.06 Response Plan for Cybersecurity Incidents.

4.5 All other incidents shall be reported to the IR Department, which will ensure that the incidents are reported in accordance with System requirements.

CONTACT: Information Resources Department Head, 979/458-6609