

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.06 Response Plan for Cybersecurity Incidents** | **Revised: May 20, 2021** |

1. GOVERNING REGULATIONS

1.1 The Federal Trade Commission provides consumer, business and law enforcement resources on its [Identity Theft](http://www.ftc.gov/bcp/edu/microsites/idtheft/) web site.

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

1.3 Administrative Procedure [50.01](https://tfsfinance.tamu.edu/modules/finance/admin/admin_procedures/5001%20Resp%20for%20Electronic%20Info%20Resources.docx) Responsibilities for Electronic Information Resources

2. DEFINITIONS

2.1 *Data security breach* is defined as any unauthorized acquisition, loss or theft of personally identifiable information maintained by Texas A&M Forest Service (TFS).

2.2 *Personally identifiable information* includes, at a minimum, an individual’s name in combination with a social security number, a driver license number, a bank account number, a credit or a debit card number, medical information or health insurance information. Personally identifiable information is considered confidential information. See Administrative Procedure 50.01 Responsibilities for Electronic Information Resources.

2.3 *Ransomware* is defined as a type of malicious software designed to block access to a computer system until a sum of money is paid.

3. PURPOSE

This procedure provides a plan that will ensure quick and efficient response to a data security breach or ransomware attack. The plan guides the response team in the damage assessment, recovery, notification and communication processes following a cybersecurity incident.

4. CYBERSECURITY INCIDENT DETERMINATION

4.1 When notified of a possible data security breach or ransomware attack, the Information Resources (IR) Department conducts a preliminary investigation to determine if such a breach or attack has occurred. The investigation identifies what happened and how and when it was detected.

4.2 If a data security breach has occurred, the IR Department ascertains when the breach occurred and if there are any fraud patterns.

4.3 If a ransomware attack has occurred, the IR Department ascertains if exfiltration of any data happened before the system was encrypted.

5. RESPONSE TEAM

When a cybersecurity incident occurs, the IR Department Head assembles a response team including appropriate staff from the IR Department, AgriLife Human Resources (HR) Department, AgriLife Information Security Officer (ISO), The Texas A&M University System (System) Security Operations Center (SOC) and TFS Director’s Office (communications staff).

6. DAMAGE ASSESSMENT

The IR Department conducts a damage assessment to determine:

6.1 Computer systems affected.

6.2 Type of cybersecurity incident – Data breach of social security numbers, credit card numbers, financial data, health information, etc. or ransomware attack.

6.3 Number of individuals affected.

6.4 List of compromised computing resources accounts.

6.5 Any indication of improper use of data.

6.6 Cost to repair the damage or recover the data.

7. RECOVERY

The IR Department is responsible for recovery operations. Based on the nature of the data security breach and the damage assessment, the IR Department determines and implements appropriate recovery operation steps or playbooks.

8. NOTIFICATION

8.1 One or more of the following individuals or groups are notified of a cybersecurity incident in accordance with System requirements.

1. Chancellor’s Office
2. System Chief Information Officer (SCIO)
3. System Chief Information Security Officer (SCIO)
4. Security Operations Center (SOC)
5. TFS Chief Information Officer (CIO)
6. AgriLife ISO
7. Affected people (employees, public)
8. System Office Marcom
9. System Internal Audit
10. Department of Information Resources (DIR)
11. Law Enforcement
12. Office of Civil Rights

8.2 For data security incidents specifically, one or more of the following individuals or groups must also be notified:

1. Executive Secretary, System Board of Regents
2. Vice Chancellor, Texas A&M AgriLife
3. Vice Chancellor of Marketing and Communications
4. Texas A&M University (TAMU) Police Department
5. Social Security Administration Fraud Line
6. Office of the Attorney General
7. Major credit bureaus:
   1. Equifax
   2. Experian
   3. Trans Union

8.3 Individuals whose personal information may have been compromised are notified in a timely manner so they can quickly take steps to rectify the situation.

9. COMMUNICATION

9.1 Any information that will hamper a criminal investigation or that will give additional information to those who might do harm will not be disclosed.

9.2 All external communications, written and verbal, are approved by the Associate Director for Finance and Administration.

9.3 Written communications will follow the tips from the System or the guidelines from the Federal Trade Commission.

9.4 The IR Department will create and maintain a web-site to announce data security breach incidents and to communicate with the media and the public.

9.5 Prior to posting, all press releases are approved by the Director.

9.6 All inquiries from the media and the general public are handled through the Communications Manager.

CONTACT: [Information Resources Department Head](mailto:cbryan@tfs.tamu.edu), 979/458-6607