

	MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE Offices of the County Executive-101 Monroe Street-Rockville, Maryland 20850	NO. 6-7 PAGE 1 of 3 DATE: 8/1/19
Title	Information Security	

1.0 Purpose

To establish an Administrative Procedure (AP) for the Users of the County's Information System(s) to ensure that the County's Information System(s) is used and administered in a manner that protects it from unauthorized or inadvertent access, use, destruction, modification, disclosure, theft, or denial of service.

2.0 Definitions

- 2.1 Compliance-Mandated Departments or Information Systems – Departments or Information Systems that process, store, and/or transmit data subject to security restrictions imposed by the Federal and State governments, Health Insurance Portability and Accountability Act (HIPAA), FBI Criminal Justice Information Services Division (FBI CJIS), and the Payment Card Industry Data Security Standard (PCI-DSS).
- 2.2 Department of Technology Services (DTS) – An Executive Branch department responsible for County Government enterprise information systems and telecommunications.
- 2.3 Enterprise Information Security Office EISO – An office within DTS that is responsible for the security of the County's Information System(s).
- 2.4 Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- 2.5 Information System Registry a central repository containing information on Information System(s).
- 2.6 Users – Individual or (system) process acting on behalf of an individual, authorized to access a system.
- 2.7 Using Department ("Department") – a department or office that owns or uses an Information System.

3.0 Policy

- 3.1 Montgomery County Government will implement security policies following security controls and associated assessment procedures defined in the most current revision of NIST SP 800–53 Recommended Security Controls for Federal Information Systems and Organizations, as adapted for County use.
- 3.2 Users must review and abide by the AP 6–7 Information Security Rules of Behavior Handbook. The handbook describes the rules associated with user's responsibilities in the use of an Information System.
- 3.3 All Departments, System owners, and data owners must review and abide by the AP 6–7 Information Security System and Data Owners Handbook, and must develop, document, and disseminate to their departments' Users procedures that implement this Administrative Procedure and associated Handbooks.
- 3.4 Compliance-Mandated Departments, System owners, and data owners must use this Administrative Procedure as baseline policy, and develop, document, and disseminate to their users Information System policies and procedures based on compliance specific guidelines. The policies and procedures must be managed by a designated official within the Department.
- 3.5 DTS must maintain and publish the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook addressing the following NIST SP 800–53 Recommended Security Controls families:
 - 3.5.1 Information Access Control
 - 3.5.2 Information Security Awareness and Training
 - 3.5.3 Audit and Accountability
 - 3.5.4 Information Security Assessment, Authorization and Monitoring
 - 3.5.5 Configuration Management

	MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE Offices of the County Executive-101 Monroe Street-Rockville, Maryland 20850	NO. 6-7 PAGE 2 of 3 DATE: 8/1/19
Title	Information Security	

- 3.5.6 Contingency Planning
- 3.5.7 Identification and Authentication
- 3.5.8 Incident Response
- 3.5.9 Maintenance
- 3.5.10 Media Protection
- 3.5.11 Physical and Environmental Protection
- 3.5.12 Planning
- 3.5.13 Personnel Security
- 3.5.14 Risk Assessment
- 3.5.15 System and Services Acquisition
- 3.5.16. System and Communication Protection
- 3.5.17 System and Information Integrity
- 3.5.18 Program Management
- 3.5.19 Exemption from Administrative Procedure
- 3.6 Exemptions – Any deviations from this policy, including Information Security Rules of Behavior Handbook and Information Security System and Data Owners Handbook, require an Exemption Request to be submitted in writing by the Using Department and approved in by DTS EISO. The request must describe a) the business case justification, b) compensating controls, c) duration, and d) the specific user, system, or application to be exempted. DTS EISO must track and report on exemptions granted.
- 3.7 Information System Registration – Using Departments must register all Information Systems with DTS and keep the registry updated at all times.
- 3.8 Information System Authorization – A Risk Assessment must be performed and approved by DTS, before any new Information System is put in production. Periodic Risk Assessments must be performed for existing Information Systems, as determined by DTS. Operations of any Information System not approved by DTS must have an approved exemption or be removed from operations.
- 3.9 Violation of this procedure is prohibited and may lead to disciplinary action, including dismissal, and other legal remedies available to the County. A County employee who violates this administrative procedure may be subject to disciplinary action, in accordance with Montgomery County law and executive regulations, including without limitation, the Personnel laws and regulations, the Ethics Laws, currently codified at Chapter 33, COMCOR Chapter 33, and Chapter 19A of the County Code, respectively, and applicable collective bargaining agreements, as amended.
- 3.10 In any contract where a contractor or business partner may have remote access to, or otherwise work or interface with, Information System(s), the following language, or language of similar import, must be included in the solicitation document and the contract, and AP 6–7 must be attached:

The Contractor may be afforded remote access privileges to Information Systems, or otherwise work on or interface with Information Systems, and must ensure that the Information Systems, including electronic data assets, are protected from unauthorized or inadvertent access, use, destruction, modification, disclosure, theft, or denial of service. The Contractor must adhere to the County's Information Security Procedure (AP 6–7), which is attached to, incorporated by reference into, and made a part of this contract.

4.0 Responsibilities

	MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE Offices of the County Executive-101 Monroe Street-Rockville, Maryland 20850	NO. 6-7 PAGE 3 of 3 DATE: 8/1/19
Title	Information Security	

4.1 User – User uses Information System(s) for County business purposes only and in compliance with this administrative procedure.

4.2 Department

- 4.2.1 Ensures users participate in the County's Information Security Awareness Training Program and comply with the County's information technology security procedures including this administrative procedure and the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook.
- 4.2.2 Enunciates department-specific information security policies and procedures and train users on them.
- 4.2.3 Reviews and updates department-specific information security policies and procedures annually.
- 4.2.4 Incorporates this administrative procedure in contracts if a contractor's employees or its agents are provided access to the Information Systems.
- 4.2.5 Cooperates with DTS in the vulnerability testing and remediation process of department-operated Information Systems assets.
- 4.2.6 Reports security incidents per procedure and assist in their investigation and prevention.
- 4.2.7 Assists DTS with maintaining Information Systems in compliance with this administrative procedure.
- 4.2.8 Ensures that all Information Systems are registered with DTS and updated annually.
- 4.2.9 Reports on compliance to handbooks as referenced in the **Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook.**

4.3 DTS

- 4.3.1 Provides information security awareness training.
- 4.3.2 Reports Information Security risk and compliance status to the CAO.
- 4.3.3 Advises Departments on information security issues.
- 4.3.4 Assists Departments in the remediation of identified vulnerabilities.
- 4.3.5 Advises Departments in the secure design of Information Systems.
- 4.3.6 Periodically conducts security scans and vulnerability testing to identify vulnerabilities.
- 4.3.7 Leads investigations and responses to Information System security incidents.
- 4.3.8 Monitors Information System security threats and manages countermeasures.
- 4.3.9 Reviews Information System solicitations/contracts for inclusion of Information Security procedure and policy.
- 4.3.10 Performs/Evaluates Risk Assessments for all new Information Systems, and periodically for all existing Information Systems identified as critical/sensitive by the Using Department and or DTS.
- 4.3.11 Maintains and implements enterprise Information System security measures; reviews and updates information security policies and handbooks.
- 4.3.12 Manages the exemption process.
- 4.3.13 Monitors and reports on Data Owners' and Departments' compliance with this AP.

5.0 Departments Affected

All Executive Branch departments and offices

6.0 Appendices

Information Security Rules of Behavior Handbook

Information Security System and Data Owners Handbook