Management Directive

Commonwealth of Pennsylvania
Governor’s Office

Management Directive 245.18 Amended – IT Administrator Acceptable Use, Auditing, and Monitoring

Date: March 14, 2023

By Direction of: Neil R. Weaver, Secretary of Administration

Contact Agency: Office of Administration
Information Technology
Telephone 717.787.5440
Email: ra-ITCentral@pa.gov

This directive sets forth policy and responsibilities for Information Technology (IT) Administrators regarding acceptable uses of Commonwealth IT Resources and their role to prevent misuse or abuse of these resources.

1. PURPOSE.

To establish the ethical and acceptable use of Commonwealth IT Resources by Application, Database, Network, and System Administrators and detail the auditing and monitoring procedures that will be employed to ensure that Administrators do not misuse their authority.

2. SCOPE.

This directive applies to all Administrators in departments, offices, boards, commissions, and councils under the Governor’s jurisdiction (hereinafter referred to as “agencies”).

3. OBJECTIVE.

To ensure Administrators understand their role in relation to privileged access to Commonwealth applications, databases, networks, and systems.

4. DEFINITIONS.

a. **Administrator.** An Authorized User with elevated privileges who is responsible for the maintenance, configuration, or operation of a computer system(s), application(s), database(s), or network(s).

b. **Application Administrator.** An Administrator responsible for the design and management of one or more applications and for the evaluation, selection and implementation of applications and associated systems.

c. **Authorized Users.** Commonwealth of Pennsylvania employees, contracted resources, consultants, volunteers, or any other users who have been granted access to and are authorized by the Commonwealth to use Commonwealth IT Resources.

d. **Database Administrator.** An Administrator responsible for the design and management of one or more databases and for the evaluation, selection and implementation of database management systems.

e. **IT Resources.** Equipment or interconnected systems or subsystems of equipment, networks, or services used to receive, input, store, process, manipulate, control, manage, transmit, display and/or output information, including, but not limited to: computers, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, Intranet, email, ancillary equipment, software, firmware, cloud-based services, systems, networks, platforms, plans and data, training materials and documentation and social media websites.

f. **Network Administrator.** An Administrator who manages a communications network. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

g. **Privileged Accounts.** Accounts that have virtually unlimited access to all programs, files, and resources on a computer system.

h. **System Administrator.** An Administrator who manages the computer systems. Responsibilities include operating system and hardware installations and configurations and may be involved with application installations and upgrades.

5. POLICY.

Security of the Commonwealth's IT systems remains vital to ongoing operations and business continuity of the Commonwealth. In addition to the expectations of an Authorized User as outlined in *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, Administrators are also expected to abide the requirements in Enclosure 1*, Acceptable Use Policy for Application, Database, Network, and System Administrators.*

Administrators are provided with privileges above and beyond what is expected of them as an Authorized User under *Management Directive 205.34 Amended*. Administrators are required to manage, configure, and monitor Commonwealth IT Resources. Administrators also have the ability to create, access, modify and/or delete electronic resources, data and systems configurations within a given technology discipline as well as grant permissions to other individuals commensurate with their own privileges in a given technology discipline. Because Administrators are trusted with rights and privileges beyond those granted to normal Commonwealth system users (Users) they must adhere to the highest standards of ethical conduct in the use of and administration of Commonwealth IT Resources. Failure to protect the integrity or the security of the network, or misuse of administrative authority, is grounds for an immediate suspension of Administrator privileges and may result in additional actions up to and including removal from employment. Administrators are required to sign the *Acceptable Use Policy Agreement for Application, Database, Network, and System Administrators*, which is attached to this directive as Enclosure 1.

In addition, Administrators will be subjected to stringent auditing and monitoring of their activities to maintain the highest level of internal security. Enclosure 2*, Auditing and Monitoring of Administrators*, which is attached to this directive, provides details on this process and the activities monitored for Administrators. Auditing and monitoring shall be performed by a security business unit separate from the infrastructure and operations personnel tasked with maintaining the health and security of the enterprise infrastructure. The separation of duties shall be utilized to avoid a potential conflict of interest or the appearance of a conflict of interest. This process is intended to provide validation and confidence in the health and security of the Commonwealth's infrastructure and information systems.

6. RESPONSIBILITIES.

a. Administrators shall:

(1) Fulfill their roles as defined above for their particular specialty.

(2) Follow all Commonwealth policies related to their roles.

(3) Report any and all misuse of Commonwealth IT Resources or administrative privileges to their supervisor or manager as the misuse is identified.

(4) Report any security incidents, or suspected security incidents as established in ITP–SEC024 – IT Security Incident Reporting Policy.

b. Supervisors and Managers shall:

(1) Ensure compliance with Commonwealth policies and training requirements.

(2) Follow through on reports of misuse of Commonwealth resources or administrative privileges as appropriate.

(3) Report any security incidents, or suspected security incidents as established in ITP–SEC024 – IT Security Incident Reporting Policy.

This directive replaces, in its entirety, *Management Directive 245.18,* dated February 7, 2006.

Enclosure 1 **Acceptable Use Policy Agreement for Application, Database, Network, and System Administrators**

Enclosure 2 **Auditing and Monitoring IT Administrators**

Enclosure 1

Acceptable Use Policy Agreement for Application, Database, Network, and System Administrators

Administrators of Commonwealth IT Resources must abide by the following:

1. Adherence to the standards set forth in *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy.*

2. Performance of activities deemed necessary to support the overall health, availability, integrity, and security of:

a. Servers, desktops, and laptops owned or controlled by the Commonwealth.

b. Network and infrastructure systems owned or controlled by the Commonwealth.

c. Physical and electronic security systems owned or controlled by the Commonwealth.

d. Database and application systems owned or controlled by the Commonwealth.

3. Guarding against corruption, compromise, or destruction of Commonwealth IT Resources and information assets.

4. Maintaining and applying all system patches and system updates, considering the expense of applying the patch, the expense of recovering from a failed patch and the likelihood that not applying a given patch will result in a security breach.

5. Taking reasonable and appropriate steps to ensure that all hardware and software license agreements are faithfully executed on all systems, networks, and servers.

6. Ensuring agency network addresses are assigned only to those entities or organizations that are part of the agency. Administrators shall not assign network addresses to non-agency entities or organizations without the specific written approval of the agency Information Security Officer (ISO).

7. Limiting access to root, administrative, service, or privileged supervisory accounts (Privileged Accounts) on Commonwealth IT Resources to Administrators only. Users shall not be given access to Privileged Accounts without the specific approval of the agency ISO. Privileged Accounts must be used only for the purposes for which they were authorized and only for conducting Commonwealth business.

8. Ensuring that default passwords shipped with servers, operating systems, databases, network equipment, or software applications are changed using strong password methodologies when the resource is installed or implemented.

9. Never sharing personal or privileged account logins or passwords with anyone including other Administrators without the approval of the agency ISO.

10. Performing all regular Commonwealth activity under a personal account and not through a Privileged Account. Non-Privileged Accounts shall be used for logging into computer resources and Administrative accounts shall only be used for operations that require elevated privileges.

11. Never knowingly creating pathways that allow for violations of network security.

12. Never gaining unauthorized access to a system (or area of a system) using knowledge of access abilities gained during a previous position at another agency or institution.

13. Never giving access on a system you do not administer to another user.

14. Always logging off or appropriately securing sessions with Privileged Account access to a point that requires a new log-on whenever leaving your work area.

15. Treating the files of system users as private unless there is reason for suspicion such as hacking, sending illegal material, etc. Administrators routinely monitor and log general usage data. When problems become apparent, they may review this data for evidence of violation of law or policy as directed by the agency respective ISO point of contact. When necessary, they may monitor all the activities and inspect the files of specific users on their IT Resources. If there is reason for suspicion, agency legal counsel and the agency respective ISO point of contact must be contacted before any action is initiated.

16. Respecting the privacy of electronic communication. Administrators shall not obtain or intercept or attempt to obtain or intercept any electronic communication or information not intended for them unless such activities are performed as part of their authorized job duties. Administrators have the duty to the owners of the information to protect the confidentiality of all such information. This includes making changes to, ensuring unauthorized users do not have access to, and not divulging to a third party that information.

17. Ensuring that all network activities tracked are complete for all users. Administrators may not single out individual users for tracking or logging, unless directed to do so by the agency human resource office and/or agency legal counsel. All users must be tracked or logged equally. To ensure the integrity of procedures and policies of network administration or to ensure network security, additional or extra activities of the Administrators may be tracked.

18. Shall not take action to disable, remove, bypass, or reverse established security controls or risk mitigation measures on IT Resources without consultation with the Agency ISO or equivalent.

19. Never engaging in any illegal or inappropriate use of Commonwealth IT Resources or engaging in activities that interfere with or disrupt network users, services, or equipment. Illegal use shall be defined as use which violates local, state, or federal law as well as Commonwealth or agency IT policy. Inappropriate use shall be defined as a violation of the goals, purpose and intended use of the network. This includes, but is not limited to, the following: stalking others, supporting partisan political activities, transmitting, or originating any unlawful, fraudulent, defamatory, or obscene communications, or any communications where the message or its transmission or distribution, would constitute or would encourage conduct that is a criminal offense or would give rise to civil liability. Interference or disruption includes, but is not limited to, distribution of unsolicited advertising or mass mailings, “spamming,” or propagation of computer worms or viruses.

20. Shall ensure that IT security training requirements set forth in *Management Directive 535.09 Amended, Information Technology Security Trainings* are met in accordance with policy.

EMPLOYEE ACKNOWLEGEMENT.

I have read and understand the Acceptable Use Policy Agreement for Application, Database, Network, and System Administrators. I will adhere to the established policy and understand if I violate the rules explained herein, I may be subject to disciplinary action, up to and including termination of employment.

Name (Print):____

Signature:______________________________ Date:________________________

Enclosure 2

Auditing and Monitoring of Administrators

This enclosure outlines the activities that should be monitored for Administrators. Please note, the central Administrators will not monitor agency Administrators. The monitoring of agency Administrators is the responsibility of the agency ISO. The monitoring of central Administrators will be done by the Enterprise Information Security Office (EISO).

1. The following is a list of sensitive activities that should be monitored:

- **a.** Unauthorized access, deletion, creation and/or modification of Commonwealth's IT applications, data, or networks.
- **b.** Unauthorized account creation, modification, or deletion.
- **c.** Creation of unauthorized entry or access points into the Commonwealth's IT Resources.
- **d.** Unauthorized transfer or access of data or information within the Commonwealth's IT Resources.
- **e.** Unauthorized transfer or access of data or information outside of the Commonwealth's IT Resources.
- **f.** Use of another individual's credentials.
- **g.** Malicious attempts to jeopardize the health of the Commonwealth's IT Resources.
- **h.** Attempts to conceal malicious or unauthorized activity.

2. **Monitoring sensitive activities.** The monitoring (or "health-checking") process gathers information about the security state of the repository service infrastructure, which includes the directory database, domain controllers, and administrative workstations for service administrators. The purpose of this monitoring is to ensure that there is no unauthorized activity (as mentioned above in #1) or misuse of administrative authority by an Administrator on Commonwealth IT Resources.

3. The Commonwealth will leverage monitoring software to collect and interpret this status. In addition, the Commonwealth has numerous domain controllers and administrative workstations, which can best be supported by compiling status information in a common database. After the information is centralized, it can be reviewed to monitor the security status of the repository as a whole.

4. **Event notification.** The monitoring described below is for the purpose of detecting security-sensitive configurations and not for the purpose of detecting intrusions. With event notification, thresholds are defined for changes in the directory service, domain controller configuration, or other repository infrastructure characteristics. When one of these characteristics changes enough to exceed the threshold, an event notification is generated, indicating a potential security breach.