SACRAMENTO COUNTY

Department of Technology

**Policy Title:** **Privileged Account Use Policy**

**Authority:** **DTech Executive Management**

**Effective Date:** **March 20, 2017**

**Purpose:**

This policy informs authorized individuals of the obligations and responsibilities which accompany priviledged access to servers and services on the County of Sacramento Wide Area Network (CoSWAN). Authorized individuals are persons who have been given permission to access a resource by the governing entity of that resource. Privileged access, commonly referred to as, administrator, admin, or root access, allows an individual full permission to the resources within their authority and/or advanced priviledges beyond those given to most users. It is a standard practice to elevate privilege levels for individuals, such as systems administrators, network administrators, database administrators, application developers, and desktop support staff to complete the work they are assigned. An individual may have access to network devices, file servers, application servers, user accounts and user data, financial data, personnel data, or desktop operating systems.

**Scope:**

This policy applies to all Sacramento County employees who maintain a privileged account on CoSWAN.

**Policy:**

1. Privileged access shall only be granted to authorized individuals.

2. Authorized individuals with privileged access must:
    a. Respect their functional access authority limits;
    b. Respect the rights of the system users;
    c. Respect the integrity of the systems and related resources they have access to;
    d. Comply with all relevant laws, policies, and regulations;

3. Authorized individuals have an obligation to familiarize themselves with all procedures, business practices, and operational guidelines pertaining to the administration of computing resources they are authorized to use or administer.

4. Employees with privileged access will use their normal Active Directory logon with multi-factor authentication to access the Privileged Account Management (PAM) system..

5. Employees with privileged access shall not share their logon or authentication credentials with anyone. Accounts with priviledged access will not be used for normal day-to-day activities.

6. All privileged accounts and their passwords will be controlled and managed through the use of Sacramento County's PAM system.

7. Authorized individuals will manage all technology resources through the PAM interface and agree to the logging, monitoring and reporting of policy compliance.

8. The request for, creation of, and compliance within privileged accounts will be according to the Technology Department's security policies and procedures.

9. Each authorized individual will read and sign the "Acknowledgement of Security Responsibility and Acceptable use of Elevated IT Privileges" agreement prior to gaining system access through PAM.

10. Non-Compliance with this poicy may subject the violator to disciplinary actions and/or penalities stipulated in applicable County policy, state, and/or federal statutes.

11. In the event that PAM does not function as intended on a given system, the CIO, or designee, may grant an exception on a case by case basis.

**Approved by:**

Rami Zakaria, CIO