CITY OF SPOKANE ADMINISTRATIVE POLICY AND PROCEDURE	ADMIN 5300-26-10 LGL 2026-0018
TITLE: USER SYSTEM ACCESS EFFECTIVE DATE: March 3, 2026 REVISION EFFECTIVE DATE: N/A	

1.0 GENERAL

1.1 This User Access Policy is established to manage and secure access to all software systems used by the City of Spokane, encompassing those hosted on-premises, in the cloud, and by third parties. It applies to all employees, contractors, and affiliated service providers of the city.

1.2 TABLE OF CONTENTS

2.0 DEPARTMENTS/DIVISIONS AFFECTED

This policy shall apply to all City divisions and departments except the Spokane Public Library.

3.0 REFERENCES

NIST Cybersecurity Framework 2.0

CIS Critical Security Controls

4.0 DEFINITIONS

4.1 Multifactor Authentication (MFA): A security mechanism that requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or a Virtual Private Network (VPN). MFA combines two or more independent credentials: what the user knows

(password), what the user has (security token), and what the user is (biometric verification).

4.2 Role-Based Access Control (RBAC): Based on a user's role within the organization, permissions are granted according to predefined roles, ensuring users have access only to the resources necessary for their job functions.

4.3 The principle of least privilege requires that all users, systems, and programs have only the minimum level of access necessary to perform authorized tasks. This security principle is intended to limit potential damage if accounts are compromised or misused.

4.4 Segregation of Duties (SoD) is a key control that prevents conflict of interest, fraud, and error. This is achieved by ensuring that no single individual has control over all phases of a transaction, making it necessary for multiple individuals to complete critical tasks or transactions.

4.5 Criminal Justice Information (CJI) is the term used to refer to all Federal Bureau of Investigation (FBI) provided data necessary for law enforcement and civil agencies to perform their missions including but not limited to biometric, identity history, biographic, property, and case/incident history data. CJI in Washington State additionally protects data that is transmitted by the Washington State Patrol and Washington State Department of Licensing.

4.6 Criminal Justice Information Services (CJIS) is a division of the Federal Bureau of Investigation (FBI) in the United States that provides information services to support law enforcement agencies at the federal, state, and local levels.

4.7 Shared Account: An account that is used by multiple individuals to access systems or data.

4.8 Administrator Account: A user account with elevated privileges, typically used for system administration tasks. This account can perform actions that affect the entire system, such as installing software, managing user accounts, configuring settings, and accessing all files and data on the system.

4.9 Service Account: A non-human account created to run specific applications or services. These accounts have permissions tailored to their specific purpose, often with limited access to ensure they only perform their intended functions.

4.10 System Testing Account: An account used for testing and quality assurance purposes. These accounts may have special permissions to simulate different user roles and test various system functionalities.

4.11 Contractor and Vendor Accounts are accounts created for individuals or organizations providing temporary services or products to the city. These accounts are granted access to specific systems or data necessary to fulfill their contractual obligations.

4.12 Active Directory (AD): Directory service developed by Microsoft for Windows domain networks. It is used for managing permissions and access to network resources. AD stores data as objects, which can include users, groups, computers, printers, and more, and organizes them into a hierarchical structure. This structure consists of domains, trees, and forests, which help organize and manage the network resources efficiently. Active Directory provides essential services such as authentication, authorization, and directory services, allowing administrators to manage and secure the network by setting policies and permissions for users and devices. It is a critical component for enterprise environments to centralize and streamline network management.

5.0 POLICY

5.1 PASSWORD POLICY

5.1.1 Password Length: Minimum of 12 characters for all users.

5.1.2 Complexity Requirements: Must include at least one uppercase letter, one lowercase letter, one number, and one special character.

5.1.3 Password History and Reuse: No reuse of the last 10 passwords.

5.1.4 Password Expiry: Mandatory change every 90 days.

5.2 ACCOUNT LOCKOUT AND PASSWORD RESET

5.2.1 Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute period.

5.2.2 Lockout Duration for invalid logon attempt(s) of 15-minute period required for CJIS applications and 5-minute period for computer systems.

5.2.3 Secure Password Recovery: Requires verification using two forms of authentication.

5.3 MULTIFACTOR AUTHENTICATION (MFA)

5.3.1 MFA is required for all systems with capabilities to provide this feature either native/built-in or integrated to Active Directory.

5.3.2 MFA required for access to Criminal Justice Information Systems.

5.3.3 Authentication Methods: Combination of knowledge, possession, and inherence factors.

5.3.4 Authenticator Management: Authenticators are changed or refreshed annually or when there is evidence of authenticator compromise. Authenticators are changed for group or role accounts when membership to those accounts is changed.

5.3.5 MFA is required for all third-party SaaS applications.

5.4 APPLICATION COVERAGE

5.4.1 All Environments: Policy applies uniformly across all applications, regardless of the hosting method.

5.5 COMPLIANCE AND ENFORCEMENT

5.5.1 Yearly vulnerability assessment audits that include user access are conducted by the Information Security Office.

5.5.2 Security awareness and policy training for all users is already included in the new employee orientation, in addition, yearly information security awareness training is completed citywide by the Information Security Office.

5.5.3 Penalties: Disciplinary actions for non-compliance, aligned with legal and regulatory standards.

5.6 ROLE-BASED ACCESS CONTROL (RBAC)

5.6.1 Role Definition and Responsibilities: Specific roles defined for IT Managers, HR Managers, and Line Managers in managing user access.

5.6.2 Least Privilege: Users granted the minimum level of access necessary to accomplish assigned organizational tasks.

5.6.3 Segregation of Duties: Critical functions are divided among roles to mitigate risks.

5.7 USER ACCESS MANAGEMENT

5.7.1 Documentation: Formalized processes for new user registration, user termination, and permission changes, documented using standardized forms and embedded in the onboarding and offboarding processes.

5.8 SPECIFIC ACCESS POLICIES

5.8.1 Network Access: Defined criteria for granting access to the municipal network, including Wi-Fi and VPN.

5.8.2 Operating System and Database Access: Detailed policies for administrative and general user accounts, including specific settings for security configurations.

5.8.3 Criminal Justice Information Systems Access: Detailed policies for access to criminal justice information aligned with the FBI Criminal Justice Information Services (CJIS) Security Policy.

5.8.4 Cloud Platform Access: Defined criteria for granting access to Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS)

5.9 SHARED ACCOUNTS

5.9.1 Shared or "generic" accounts shall not be used in place of individual user accounts.

5.9.2 Service accounts with limited permissions may be created to enable restricted shared access, such as a Kiosk system.

5.10 CONTRACTOR AND VENDOR

5.10.1 All contractors and vendors shall sign a Non-Disclosure Agreement (NDA) before being granted access to any City systems or data.

5.10.2 A comprehensive list of all contractor and vendor accounts shall be maintained using Active Directory (AD) by the administrator of each AD group that includes these categories, including details of the access provided, the purpose of access, and the duration of access.

5.10.3 Contractor and vendor accounts shall automatically expire after 180 days. Extensions must be formally requested and documented, including a justification for the extended access.

5.10.4 Where feasible, all contractor and vendor accounts shall use multi-factor authentication (MFA) to enhance security.

5.10.5 Access granted to contractor and vendor accounts shall be restricted to the minimum necessary for them to perform their contractual duties. Permissions shall be reviewed regularly and adjusted as needed.

6.0 PROCEDURE

6.1 MONITORING AND REVIEW

6.1.1 User and Administrator Activity Monitoring: Regular monitoring through audit logs, with monthly reviews for suspicious activities.

6.1.2 Information Technology (IT) Department is responsible for managing access to applications and services. Exceptions must be documented, reviewed, and approved by the Chief Information Officer (CIO) or their designee.

6.1.3 Police IT is responsible for managing access to Police Department applications and services.

6.1.4 Annual Access Reviews: Systematic reviews of user access rights and permissions, ensuring alignment with current roles and responsibilities will be performed by the administrators of each active directory group.

7.0 RESPONSIBILITIES

7.1 IMPLEMENTATION AUTHORITY

The IT Division is responsible for policy enforcement in coordination with Human Resources and department heads to ensure compliance.

8.0 APPENDICES

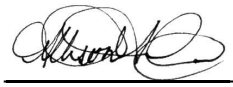
None

APPROVED BY:

Michael J Piccolo
Michael J Piccolo (Feb 27, 2026 10:37:30 PST)

Michael J. Piccolo
City Attorney

Feb 27, 2026
Date



Allison Adam
Human Resources Director

Feb 27, 2026
Date

Laz Martinez
Laz Martinez (Feb 27, 2026 12:11:04 PST)

Laz Martinez
IT Director and CIO

Feb 27, 2026
Date

Alexander Scott
Alexander Scott (Mar 3, 2026 11:49:20 PST)

Alexander Scott
City Administrator

Mar 3, 2026
Date

CITY OF SPOKANE

Final Audit Report 2026-03-03

Created:	2026-02-27
By:	Daniel Rose (drose@spokanecity.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA5lyA21KvkpYQrttr6467l8zl0d84jlq4

"CITY OF SPOKANE" History

Document created by Daniel Rose (drose@spokanecity.org)
2026-02-27 - 6:23:03 PM GMT

Document emailed to Micheal Piccolo (mpiccolo@spokanecity.org) for signature
2026-02-27 - 6:23:07 PM GMT

Document emailed to Allison Adam (aadam@spokanecity.org) for signature
2026-02-27 - 6:23:08 PM GMT

Document emailed to Laz Martinez (lmartinez@spokanecity.org) for signature
2026-02-27 - 6:23:08 PM GMT

Document emailed to Alexander Scott (ascott@spokanecity.org) for signature
2026-02-27 - 6:23:08 PM GMT

Email viewed by Micheal Piccolo (mpiccolo@spokanecity.org)
2026-02-27 - 6:36:40 PM GMT

Signer Micheal Piccolo (mpiccolo@spokanecity.org) entered name at signing as Michael J Piccolo
2026-02-27 - 6:37:28 PM GMT

Document e-signed by Michael J Piccolo (mpiccolo@spokanecity.org)
Signature Date: 2026-02-27 - 6:37:30 PM GMT - Time Source: server

Email viewed by Laz Martinez (lmartinez@spokanecity.org)
2026-02-27 - 8:10:14 PM GMT

Document e-signed by Laz Martinez (lmartinez@spokanecity.org)
Signature Date: 2026-02-27 - 8:11:04 PM GMT - Time Source: server

Email viewed by Allison Adam (aadam@spokanecity.org)
2026-02-27 - 11:56:24 PM GMT

Document e-signed by Allison Adam (aadam@spokanecity.org)

Signature Date: 2026-02-27 - 11:58:16 PM GMT - Time Source: server

Email viewed by Alexander Scott (ascott@spokanecity.org)

2026-03-03 - 7:48:34 PM GMT

Document e-signed by Alexander Scott (ascott@spokanecity.org)

Signature Date: 2026-03-03 - 7:49:20 PM GMT - Time Source: server

Agreement completed.

2026-03-03 - 7:49:20 PM GMT