CITY OF SPOKANE	CITY OF SPOKANE ADMINISTRATIVE POLICY	ADMIN 5300-18-07 LGL 2018-0019
	TITLE: ADMINISTRATOR PRIVILEGES EFFECTIVE DATE: NOVEMBER 15, 2018 REVISION EFFECTIVE DATE: N/A	

1.0 GENERAL

1.1 This policy shall establish security guidelines to ensure safe computing practices. Running a computer system with administrative privileges poses a significant risk to the confidentiality, integrity, security, and availability of the City of Spokane's information assets.

1.2 TABLE OF CONTENTS

2.0 DEPARTMENTS/DIVISIONS/VENDORS AFFECTED

2.1 Applicable to all divisions, organizations and vendors that administer technology and systems on the behalf of the City of Spokane.

3.0 REFERENCES

CIS Critical Security Control Guideline # 4 - Controlled Use of Administrative Privileges

City of Spokane's Information Security Policy

NIST Cybersecurity Framework – PR.AC-4, PR.AT-2, PR.MA-2, PR.PT-3

NERC-CIP – CIP-005-5 Cyber Security – Electronic Security Perimeters

CIP-004-5 Access Management Program

PCI-DSS v3.2 Sections 7.1, 10.2.2

RCW 19.255.020 - Liability of processors, businesses, and vendors

RCW 42.56.420 – Security

Washington State Patrol Procedure #01.01.000 - Section II, Part A

4.0 DEFINITIONS

4.1 "Administrative Privileges" is the highest level of permission that can be granted to a computer user.

4.2 "Application Administrator" is when support and maintenance occurs on an internal and/or a third party application. This includes service account rights and maintenance, writing and running database queries, analyzing database/reporting results, troubleshooting and resolving application and reporting problems.

4.3 "CIS Controls" is the Center for Internet Security Critical Security Controls for Effective Cyber Defense and is a set of actions for cyber defense that provides a specific and actionable way to thwart the most pervasive attacks. The CIS Controls are a relatively short list of high-priority, highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve cyber defense.

4.4 "CJIS" is a division of the United States Federal Bureau of Investigations that stands for Criminal Justice Information Services. CJIS is a computerized criminal justice information system that is repository for all criminal information.

4.5 "Domain Administrator" is an account granted administrative access to all computing devices within the City of Spokane's computer networks, clients and servers.

4.6 "Elevated Privileges" is when a user is granted the ability to do more than a standard user.

4.7 "Enterprise class system" is described as hardware and software designed to meet the demands of a large organization.

4.8 "Local Administrator" is when a user is granted full permissions on their assigned computing device with no other access to any other devices on the City of Spokane's networks.

4.9 "NERC-CIP" stands for North American Electric Reliability Corporation Critical Infrastructure Protection, which is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

4.10 "Network Administrator" is responsible for keeping an organization's computer network, routers, switches, and firewalls secure and running smoothly.

4.11 "NIST Cybersecurity Framework" provides a framework for computer security guidance for how organizations in the United States can assess and improve their ability to prevent, detect and respond to cyber-attacks.

4.12 "PCI DSS" stands for Payment Card Industry Data Security Standard, and is a worldwide security standards assembled by the Payment Card Industry Security Standards Council (PCI SSC).

4.13 "Standard User Account" is a basic account a user is granted for normal everyday tasks. Standard user accounts are for users who need to run applications but are restricted in their administrative access to the computer.

5.0 POLICY

5.1 It is the policy of the City of Spokane that all accounts that access technology do so with a standard user account.

5.2 Elevated account privileges shall be restricted, ensuring all elevated access is based on need-to-know and with the least amount of privileges possible.

5.3 Administrative Privileges Requirements

5.3.1 Individuals granted administrative privileges for specific business requirements shall be provided a second network account specifically for elevated computing activities.

5.3.2 Local administrative privileges on any City of Spokane computing device shall be granted only when a technical workaround is not available to allow employees to perform their role.

5.3.3 All accounts that are granted administrative privileges with elevated permissions to enterprise class systems must use Multi-Factor Authentication (MFA) while accessing administrative accounts and shall be managed with an enterprise security application.

5.3.4 Accounts with elevated privileges shall only be used for administrative activities and not for general computing tasks nor general internet access.

5.3.5 Each organization shall identify any roles within their organization with elevated privileges that require additional protection.

5.3.6 For auditing requirements, a list of all individuals that is granted administrative privileges shall be kept up-to-date at all times.

5.3.7 All employees who are granted administrative privileges shall be reviewed periodically to validate that the employee has the correct level of access.

6.0 RESPONSIBILITIES

6.1 The Information Security Officer is responsible for the annual review of the Local System Administrator Policy.

6.2 The Information Security Office will annually audit all accounts with administrative privileges within all divisions and organizations.

6.3 Domain Administrator, Application Administrator and Network Administrator Privileges shall be reviewed and approved by the ITSD Director or an appointed delegate.

6.4 All elevated access requests shall be reviewed by the user's Director and shall be approved by the ITSD Director or the appointed delegate.

7.0 APPENDICES

7.1 The justification form for Administrative Privileges is located on the city's SharePoint website. Search for City-Wide Documents. The justification form is located within the Information Technology folder.

APPROVED BY:

City Administrator — Date: 10/31/18

Director – Innovation & Technology Services Division — Date: 10/26/18

City Attorney — Date: 10/15/18

Administrative Privileges
Justification Form

Applicable to all Divisions and Vendors associated with the City of Spokane
This form is in reference to the Administrator Privileges Policy

Impact Statement:

Administrative privileges grant users complete control over most functions and features of the Operating System and Applications. Logging in or using elevated privileges on a device with administrative privileges poses a high risk to the City of Spokane's networks and data.

Please Note: Please use extreme caution when elevating up to conduct administrative privileges.

Instructions:

Justification is required for a secondary account is required for administrative privileges to be granted. Please fill out this form in detail. The director of your department must approve and sign for the justification for administrative privileges for your account. Send this completed form to the Helpdesk for final approval. *Helpdesk shall send this form to the ITSD Director for final approval.*

Please note: This justification form will be required to be completed again when a requester's job role or responsibilities is reclassified. Policy exceptions will not be renewed automatically.

EMPLOYEE INFORMATION:	
First Name:	Last Name:
Phone:	T-Number/Computer/System*:
Location:	End Date of Requested Access:

*For multiple systems access, enter "See Attachment" and attach second sheet

JUSTIFICATION FOR ADMINISTRATIVE PRIVILEGES: (PLEASE FILL OUT IN DETAIL)

APPROVALS:	
Department Director's Name (Print):	
Signature:	
Phone:	Date:

ITSD Staff Only:		
Details about permissions given:		
Reviewed By:		Initials:
Approved ☐	Disapproved ☐	Date:
ITSD Director:		
Notes:		
ITSD Director's Name (Print):		
Signature:		
Approved ☐	Disapproved ☐	Date:

Created June 2018
The IT Security Office shall administer this Justification Form