Office of the
Washington
State Auditor
Pat McCarthy

Data Backup and Disaster Recovery

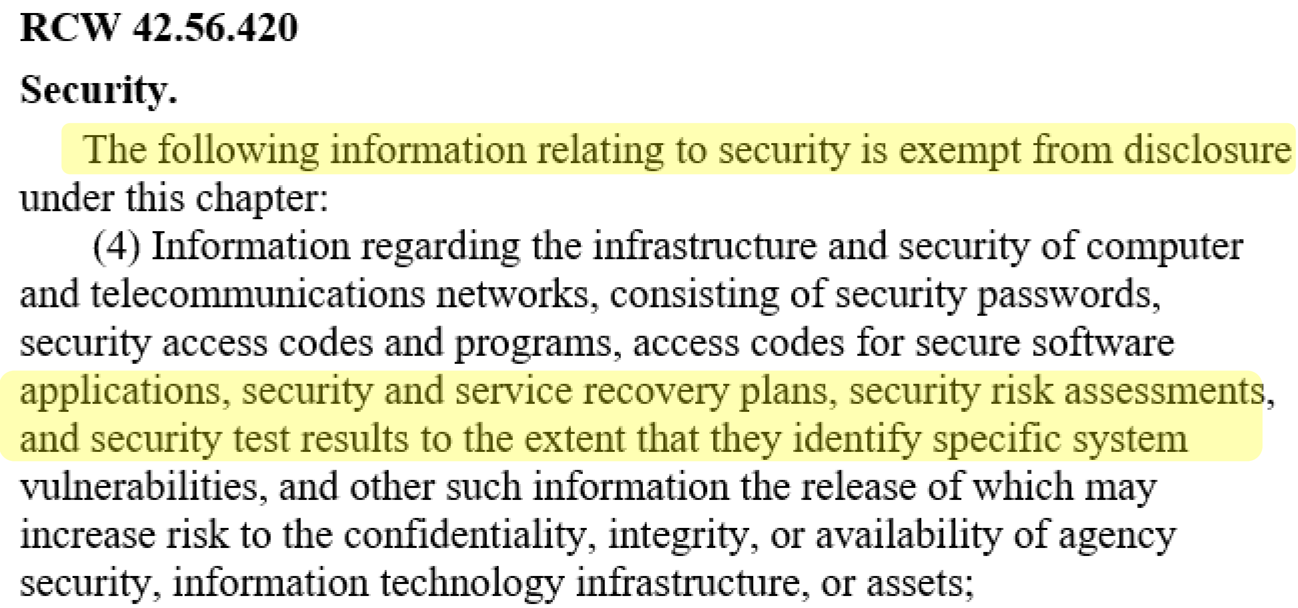
Diana Evans, *IT Auditor*

Robert Pratt, *IT Auditor*

Joint Legislative Audit & Review Committee

September 30, 2020

Protecting sensitive information



RCW 42.56.420

Security.

The following information relating to security is exempt from disclosure under this chapter:

(4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of agency security, information technology infrastructure, or assets;

Key audit findings

- Audited agencies can improve their ability to restore critical systems and data in the event of a disaster or security incident

- Audited agencies lacked the resources and guidance they needed

Audit questions

1. Have selected state agencies implemented data and system backup policies and procedures that comply with state requirements and align with best practices?

2. Do those agencies have a current, tested, disaster recovery plan that complies with state requirements and aligns with best practices?

Effective data backup and disaster recovery procedures

- Business impact analysis
  - ✓ Evaluates effects of disruptions
- IT risk assessment
  - ✓ Analyzes potential threats and likelihood

Effective data backup and disaster recovery procedures

- Data backup strategy
  - ✓ Identifies systems and data files to backup
  - ✓ Frequency
  - ✓ Backup storage location
  - ✓ Retention
- Disaster recovery plan
  - ✓ Roles and responsibilities
  - ✓ Contact information
  - ✓ Detailed recovery procedures

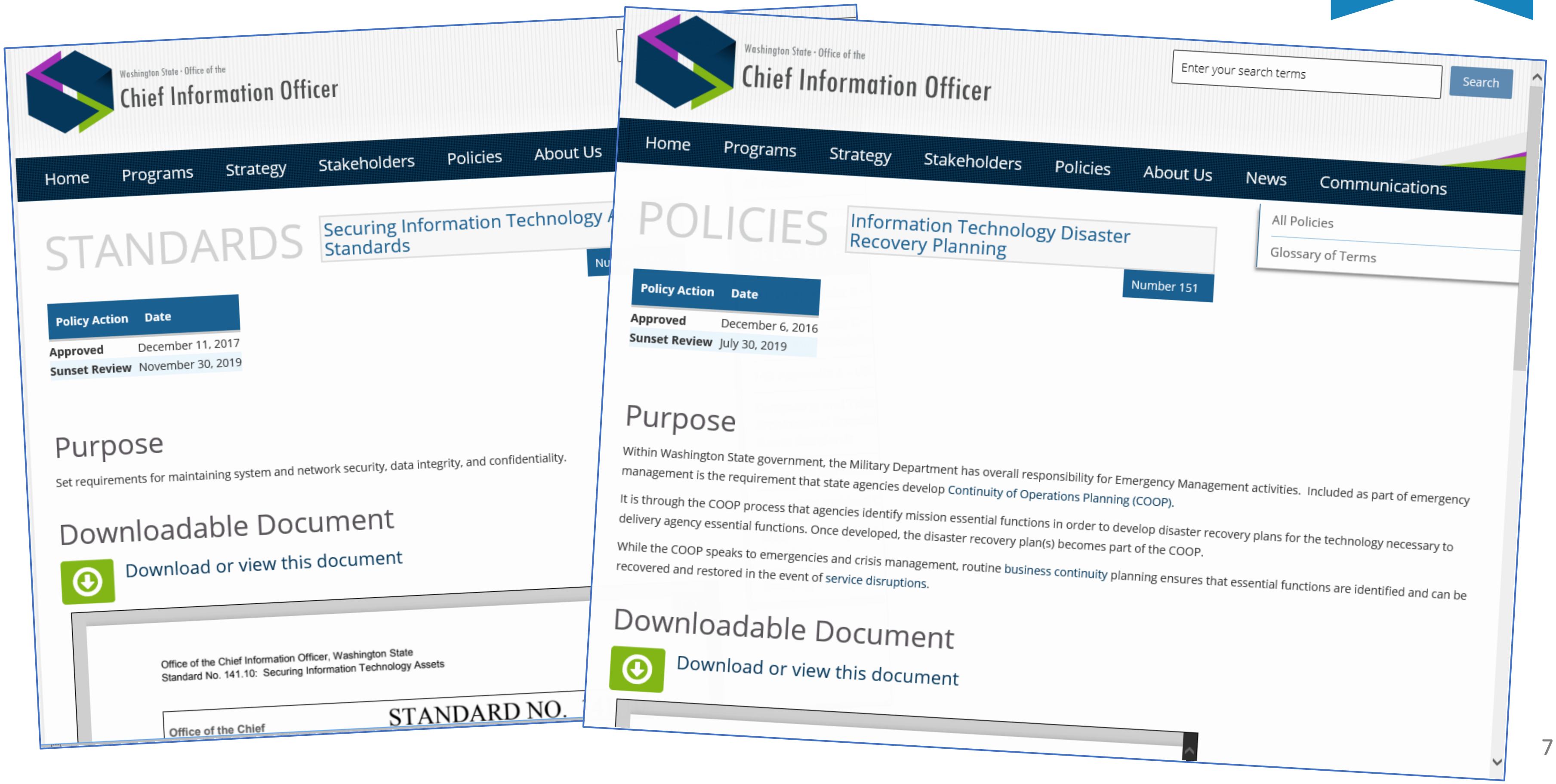
State requirements

Office of the Washington State Auditor
Pat McCarthy

Standard 141.10:
Security IT Assets, Section 8.4

and

Policy 151: IT Disaster Recovery Planning



STANDARDS

Securing Information Technology A
Standards

Policy Action	Date
Approved	December 11, 2017
Sunset Review	November 30, 2019

Purpose

Set requirements for maintaining system and network security, data integrity, and confidentiality.

Downloadable Document

Download or view this document

Office of the Chief Information Officer, Washington State
Standard No. 141.10: Securing Information Technology Assets

Office of the Chief

STANDARD NO.

POLICIES

Information Technology Disaster Recovery Planning

Number 151

Policy Action	Date
Approved	December 6, 2016
Sunset Review	July 30, 2019

Purpose

Within Washington State government, the Military Department has overall responsibility for Emergency Management activities. Included as part of emergency management is the requirement that state agencies develop Continuity of Operations Planning (COOP).

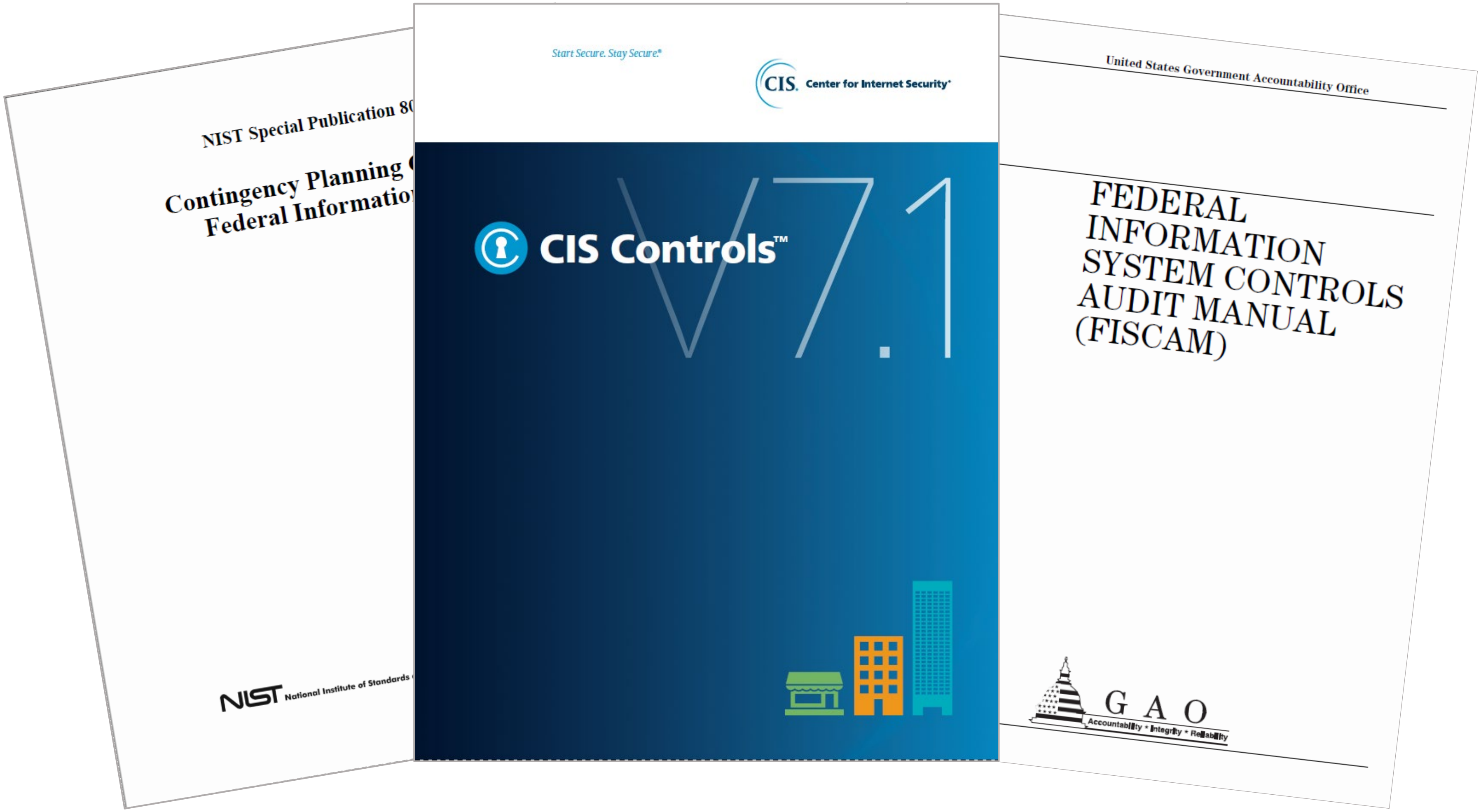
It is through the COOP process that agencies identify mission essential functions in order to develop disaster recovery plans for the technology necessary to delivery agency essential functions. Once developed, the disaster recovery plan(s) becomes part of the COOP.

While the COOP speaks to emergencies and crisis management, routine business continuity planning ensures that essential functions are identified and can be recovered and restored in the event of service disruptions.

Downloadable Document

Download or view this document

Leading practices we selected



NIST Special Publication 80

Contingency Planning G
Federal Informatio

NIST National Institute of Standards

Start Secure. Stay Secure.®

CIS. Center for Internet Security®

CIS Controls™

V7.1

United States Government Accountability Office

FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)

GAO
Accountability * Integrity * Reliability

To conduct our review

- Selected four systems and four state agencies
- Compared agency processes and procedures to ensure:
  - ➢ Data and system backups are secure and available
  - ➢ A comprehensive, tested disaster recovery plan exists

Audited agencies can improve their backup and recovery programs

None fully and consistently met all state requirements:

- Data backup
- Disaster recovery
- Testing recovery plans
  - Three of four had not performed comprehensive testing of their disaster recovery plans

Audited agencies can improve their backup and recovery programs

While not required, following backup and disaster recovery guidance offered by leading practices could help

Lacking resources

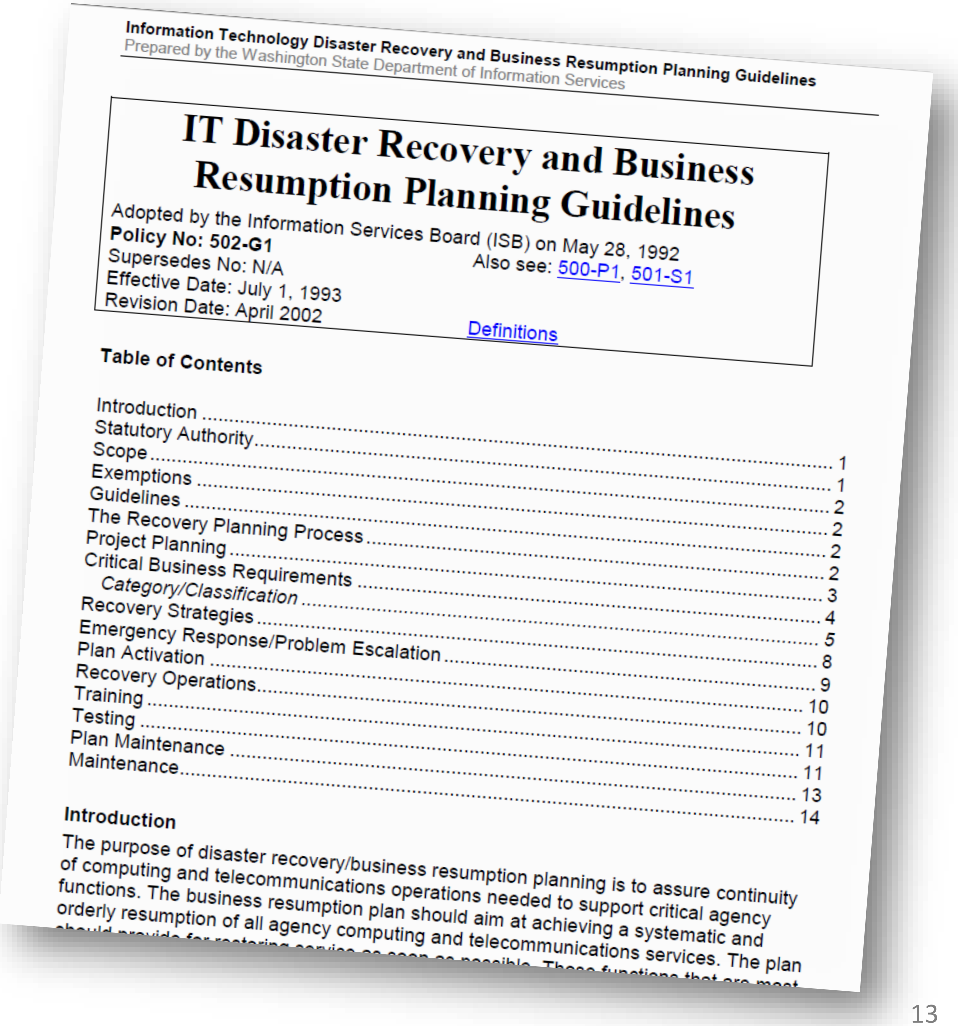
Audited agencies lacked the resources they needed

- Executive managers at some agencies:
  - Were not always aware of all risks and potential consequences
  - Did not always allocate adequate resources to address the risks
- Guidance was lacking or outdated

Better guidance needed

Better statewide guidance and tools could help with both backup strategies and disaster recovery plans

- Available guidance is:
  - Outdated
  - Hard to find on the OCIO website
- Statewide tools, such as templates, are insufficient



Information Technology Disaster Recovery and Business Resumption Planning Guidelines
Prepared by the Washington State Department of Information Services

IT Disaster Recovery and Business Resumption Planning Guidelines

Adopted by the Information Services Board (ISB) on May 28, 1992
Policy No: 502-G1
Supersedes No: N/A
Effective Date: July 1, 1993
Revision Date: April 2002
Also see: 500-P1, 501-S1
Definitions

Table of Contents

Introduction

The purpose of disaster recovery/business resumption planning is to assure continuity of computing and telecommunications operations needed to support critical agency functions. The business resumption plan should aim at achieving a systematic and orderly resumption of all agency computing and telecommunications services. The plan should provide for restoring service as soon as possible. Those functions that are most

Recommendations

We recommend the audited agencies:

- Perform and use IT risk assessments and business impact analyses to identify objectives and gaps
- Ensure executive management work closely with IT staff to consider results when allocating resources
- Further align backup and disaster recovery practices and procedures with state requirements and leading practices

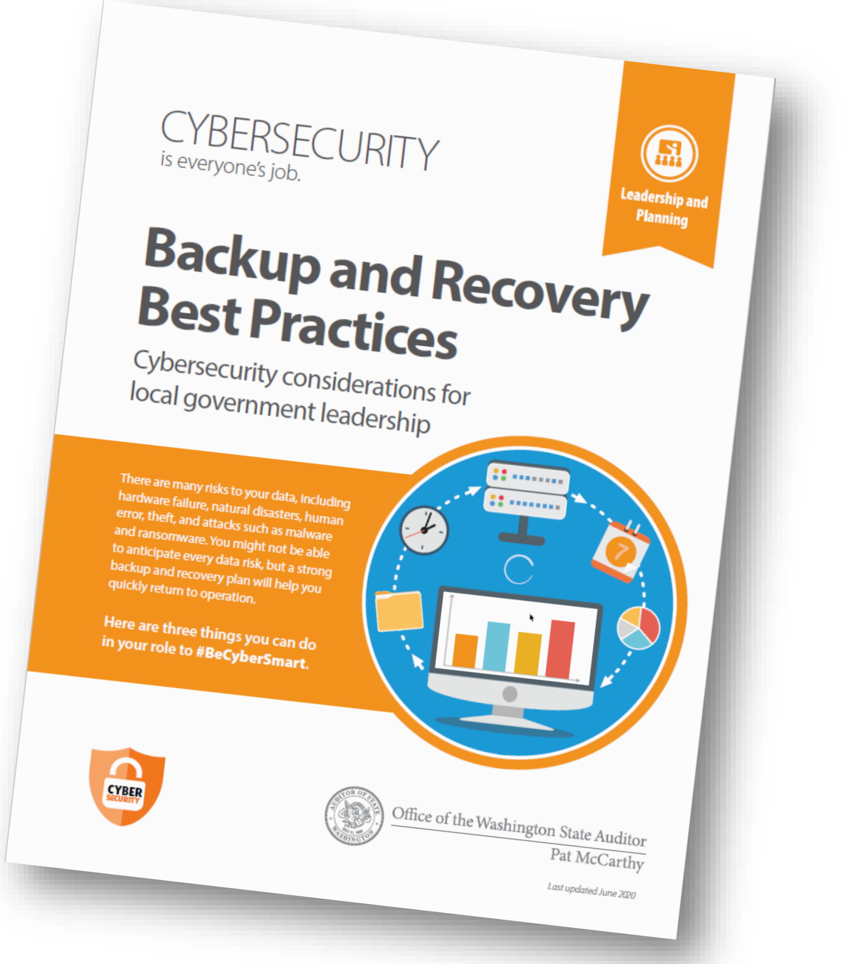
Recommendations

We recommend the OCIO:

- Update the *IT Disaster Recovery and Business Resumption Guidelines* and make them readily available to state agencies on the ocio.wa.gov website
- Offer agencies tools and templates for backup strategies and disaster recovery planning, such as IT risk assessments and business impact analyses

Applicable to all state agencies and local governments

- Other state agencies and local governments may find the recommendations from this audit helpful
- Resources on our website
  - ✓ #BeCyberSmart
  - ✓ Backup and Recovery Best Practices booklet



CYBERSECURITY
is everyone's job.

Leadership and Planning

Backup and Recovery Best Practices

Cybersecurity considerations for local government leadership

There are many risks to your data, including hardware failure, natural disasters, human error, theft, and attacks such as malware and ransomware. You might not be able to anticipate every data risk, but a strong backup and recovery plan will help you quickly return to operation.

Here are three things you can do in your role to #BeCyberSmart.

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Last updated June 2020

Questions

Contact information

Pat McCarthy

State Auditor

Pat.McCarthy@sao.wa.gov

(564) 999-0801

Scott Frank

Director of Performance & IT Audit

Scott.Frank@sao.wa.gov

(564) 999-0809

Diana Evans

IT Auditor

Diana.Evans@sao.wa.gov

(564) 999-0952

Robert Pratt

IT Auditor

Robert.Pratt@sao.wa.gov

(564) 999-0956

Website: www.sao.wa.gov

Twitter: *@WAStateAuditor*

Facebook: www.facebook.com/WAStateAuditorsOffice