

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

**Policy that describes the requirements for
all application and data servers which are
private and public – including Cloud
based applications and data**

Physical and Virtual Server Security Policy

2025



Physical and Virtual File Server Security Policy

Table of Contents

Physical and Virtual File Server Security Policy	3
Policy Purpose	3
Policy Statement.....	3
Applicability	3
Terms and Definitions.....	3
Server Requirements	4
Critical Server Requirements	4
General Server Requirements.....	4
Public Server Requirements.....	4
Server Configuration Guidelines.....	5
Ransomware Protection	6
AI Server Security Tools	7
Job Descriptions.....	8
Chief Information Security Officer	
Forms	9
Server Registration Form	
Application & File Server Inventory	
What's New	10

Physical and Virtual File Server Security Policy

Physical and Virtual File Server Security Policy

Policy Purpose

The purpose of this policy is to establish guidelines for the security and management of critical, general, and public servers hosting enterprise data and applications. This includes data and servers that are located in virtual environments (i.e. cloud). Included are all derivations of data and applications that are stored in any format or media by any users of the data and applications.

Policy Statement

Physical servers must be housed in a secure facility with 24/7 power support. Virtual servers must comply with all applicable compliance requirements and be designated for the installation of the operating system, security, and

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

emergency
dated
administrator will
the server's

Sensitive, private, and confidential data is not to be stored or back-up on public (open) servers on the cloud without a complete review and approval of the IT group, internal audit, and external auditors.

AI capabilities can provide many advantages in enhancing cybersecurity defenses. Some of the most significant benefits of AI security include: Enhanced threat detection: AI algorithms can analyze large amounts of data in real-time to improve the speed and accuracy of detecting potential cyberthreats.

Applicability

This policy applies to all servers (both data and application), system administrators, and computer systems running server operating system software connected to the enterprise network.

Terms and Definitions

- **Critical server** – a system housing sensitive or confidential data, requiring external access which serves critical business functions.
- **General server** – a system housing public data, requiring internal-only access, and serves general business functions.
- **Public server** - a server that is in the virtual environment (cloud) that can be accessed from anywhere by anyone who has access to the network (Internet).

The number of Ransomware attacks cost associate with those attacks continues to soar. It is estimated to be over \$100 billion and close to \$250 billion by 2030.



Physical and Virtual File Server Security Policy

AI Server Security Tools

AI based server monitoring is a tool that can be used to monitor, detect, communicate, respond to issues that impact the security of servers.

- Agent-based and agentless event log consolidation, backups, archiving, retention, parsing, real-time monitoring and security audit reporting
- Centrally manage all of your hardware devices with our high throughput UDP and TCP Red
- **This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.**
- **<https://e-janco.com>**
- and Office 365 audit log, sign-in log
- log management to meet all of
- itor and analyze W3C, CSV, IIS Logs,
- Windows firewall logs and any other text-base log file on both Windows and Linux
- Detect intrusions in real-time, notify and take meaningful action to automatically block active cyber-attacks and prevent new cyber-attacks

Physical and Virtual File Server Security Policy

Job Descriptions

Attached is a the following job description in a subdirectory

Chief Information Security Officer

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

Physical and Virtual File Server Security Policy

Forms

Attached are forms that are in the subdirectory named forms

Server Registration Form

Application & File Server Inventory

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

Physical and Virtual File Server Security Policy

WHAT'S NEW

2025

- Include AI security protection option
- Updated included job description
- Updated included forms

2024

- Added Section on AI Server Security Tools
- Added job description for Chief Information Security Officer CISO
- Updated included forms

2023

- Updated included forms

2022

- Updated to meet the latest ISO requirements
- Updated included forms

2021

- Updated included forms

2020

- Reviewed and updated to meet all mandated security and privacy requirements for CCPA
- Updated the included electronic forms

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>