Outsourcing & Cloud Based File Sharing Policy

Janco Associates, Inc.

2024 Edition

Table of Contents

Outsourcing Cloud-Based File Sharing Management Standard

Overview

Outsourcing and Cloud-Based File Sharing do not remove the enterprise's requirement to manage the process or the data. Even a comprehensive outsourcing and cloud-based file-sharing arrangement requires Service Level Agreement (SLA) monitoring and redefinition, as well as strategic management and other retained functions.

Standard

Service Level Agreements (SLA)

The SLA is the central instrument for managing an outsourced function. The Information Technology ~~~~~~ enforce the contract terms if an SLA is ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ ning SLAs to take into account changes

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ entity is critical to maintaining high service levels. IT will ensure that the Help Desk staff is trained to identify whether a problem lies with IT or a particular vendor. In a multi-vendor environment, this task becomes even more critical if one is to avoid a constant reassignment of the problem.

In the case of file sharing, the Help Desk Staff should be able to manage and diagnose issues associated with this technology. At the same time, they should be versed in reviewing logs and diagnostics of the vendors who provide the service.

---

[1] The web site https://www.e-janco.com has a tool kit and sample metrics that can be used for this

Security, Disaster Recovery, Business Continuity, Records Retention, and Compliance

ENTERPRISE maintains the primary responsibility for all the data and processes that are outsourced and placed in the cloud via a file-sharing process. It is for this reason that this policy needs to be followed.

All the other supporting infrastructure policies need to be followed. This includes but is not limited to the following:

- Disaster recovery and business continuity
- Security compliance and management
- Compliance management
- Backup and backup retention
- Internet, email, social networking, mobile devices, electronic communication, and records retention
- Mobile device access and use
- Physical and virtual server security
- Records management, retention, and destruction
- Sensitive information
- Social networking
- Telecommuting
- Text messaging
- Travel and off-site meetings

Outsourcing Policy

Policy Statement

The enterprise will consider the outsourcing and Cloud-Based File Sharing of parts of its Information _____ true added value. These _____ onstrates the cost-effectiveness _____ cloud-based file-sharing _____ ent (SLA). SLAs will contain clear

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

Goal

The goal of outsourcing and cloud-based file sharing is to seek areas in which vendors' convenience and economies of scale can streamline IT operations, add value, and allow the enterprise to concentrate its efforts on core competencies.

Electronic Forms

Six (6) electronic forms are included with this policy template. They come separately in their own directory.

- Outsourcing and Cloud Security Compliance Agreement

- Outsourcing Security Compliance Agreement

- Remote Location Contact Information

- Vendor Contact

- Work From Home IT Checklist

- Work From Home Work Agreement

Job Descriptions

Five (5) electronic forms are included with this policy template. They come separately in their own directory.

- Vice President Strategy and Architecture

- Manager Cloud Applications

- Manager Outsourcing

- Manager User Support

- Manager Vendor Management

- Manager WFH Support

- Cloud Computing Architect

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

Audit Program Guide

Background

All providers of medical services were required to comply with ISO 27001. ISO 27001 was created to improve the efficiency and effectiveness of all systems through the development of security standards for electronic transactions.

ISO 27001 requires that the organizations:

- Provide information to individuals about their privacy rights and how their information can be used
- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ y procedures are adopted and
- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ information, so that they are

The focus of the HIPAA audit is:

- Review of written policies and practices on security
- Review of written policies and practices on privacy
- Review of processes in practice vs. privacy policies and procedures
- Review of processes in practice vs. security policies and procedures
- Review of business associates to ensure that each has a valid contract or agreement, especially new associates or partners

ISO 27001 requirements

- Electronic transactions and code sets are secure
- Electronic information privacy
- Unique identifier for key information
- Security requirements are met
- Enforcement procedures are in place

ISO 27001 implementation requires

- Information Technology and Internet-based Privacy Inventory
- Training seminars (introductory, intermediate, and advanced)
- Privacy and security analysis and assessment
- Implementation and compliance advice
- Policies and compliance materials
- Privacy documents (e.g., consents, notices, authorizations, business associate agreements)

Top 10 Cloud and Outsourcing SLA Best Practices

1. **Define SLA roles and responsibilities for the enterprise and cloud providers**. These definitions should include, the persons responsible for oversight of the contract, audit, performance management, maintenance, and security.

2. **Define key terms**. Include definitions for dates and performance. Define the performance measures of ~~ance. These measures would include~~ ~~ss the cloud at any given time; and~~

   ~~vider~~. Include who is responsible for ~~LA Best Practices~~

   ~~vice is to be available to the~~ enterprise).

   - **Capacity and capability of cloud service** (e.g., the maximum number of users that can access the cloud at one time and the ability of the provider to expand services to more users).

   - **Response time** (e.g., how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to service outages).

4. **Specify how and when the enterprise has access to its data and networks**. This includes how data and networks are to be managed and maintained throughout the SLA and transitioned back to the enterprise in case of exit/termination of service.

5. **Specify specific SLA infrastructure and requirements methodology**:

   - How the cloud service provider will monitor performance and report results to the enterprise.

   - When and how the enterprise, via an audit, is to confirm the performance of the cloud service provider.

6. **Provide for disaster recovery and continuity of operations planning and testing**. Include how and when the cloud service provider is to report such failures and outages to the enterprise. Also, how the provider will re-mediate such situations and mitigate the risks of such problems from recurring.

7. **Describe any applicable exception criteria when the cloud provider's performance measures do not apply** (e.g., during scheduled maintenance or updates).

8. **Specify metrics the cloud provider must meet to show it is meeting the enterprise's security performance requirements for protecting data** (e.g., clearly define who has access to the data and the protections in place to protect the enterprise's data). Specify the security performance requirements that the service provider is to meet. This would include describing security performance metrics for protecting data, such as data reliability, data preservation, and data privacy. Clearly define the access rights of the cloud service provider and the enterprise as well as their respective responsibilities for securing the data, applications, and processes to meet all mandated requirements. Describe what would constitute a breach of security and how and when the service provider is to notify the enterprise when the requirements are not being met.

What's New

2024 Edition

- Updated all included job descriptions
- Updated all included forms

2023 Edition

- Added two (2) job descriptions
  o Manager User Support
  o Manager WFH Support
- Updated all included job descriptions
- Updated all included forms
- Updated remote worker requirements
- Updated included audit program

2022 Edition

- Updated all included job descriptions
- Updated all included forms
- Updated remote worker requirements
- Updated included audit program

2021 Edition

- Updated all included job descriptions
- Updated all included forms
- Added forms to support WFH
  o Added Work From Home IT Checklist
  o Added Work From Home Work Agreement

2020 Edition

- Added Work from Home Considerations
- Added Job Descriptions
  o Vice President Strategy and Architecture
  o Cloud Computing Architect
  o Manager Cloud Applications
- Updated all electronic forms
- Added electronic forms
  o Vendor Contact Form
  o Remote Location Contacts
- Updated to meet the latest compliance requirements
- Added eBook version of the policy