Docupile

SOC 2 Compliance Checklist

for Document Management Systems

Use this checklist to ensure that a document management system, like Docupile, meets SOC 2 compliance standards.

1) Security

Does the system protect against unauthorized access (both physical and logical)?

- [ ] Verify if the system uses advanced security measures like firewalls and intrusion detection systems.
- [ ] Ensure multi-factor authentication (MFA) is required.

2) Availability

Is the system accessible as stipulated by a contract or service level agreement (SLA)?

- [ ] Check if redundant systems and regular maintenance are in place.
- [ ] Verify if there is a robust disaster recovery plan.

3) Processing Integrity

Is the system accessible as stipulated by a contract or service level agreement (SLA)?

- [ ] Check if redundant systems and regular maintenance are in place.
- [ ] Verify if there is a robust disaster recovery plan.

4) Confidentiality

Is sensitive information protected from unauthorized access?

- [ ] Ensure encryption and access controls are used.
- [ ] Verify if secure data storage solutions are in place.

5) Privacy

Is personal information collected, used, retained, disclosed, and disposed of in conformity with privacy commitments?

- [ ] Check if strict privacy policies and procedures are followed.
- [ ] Verify compliance with relevant privacy regulations.

6) Regular Security Assessments

Are regular security assessments conducted?

- [ ] Check if periodic vulnerability scans and security assessments are performed.
- [ ] Ensure the system is updated based on the findings of these assessments.

7) User Training

Is ongoing training provided to personnel?

- [ ] Verify if staff receive regular training on SOC 2 regulations and best practices.
- [ ] Check if the training includes data handling procedures and security protocols.

8) Business Associate Agreement (BAA)

Is there a signed BAA with the document management provider?

- [ ] Ensure a BAA is in place to confirm the provider's compliance with SOC 2 regulations.

9) Incident Response Plan

Does the system have an incident response plan?

- [ ] Verify if there is a documented plan for responding to data breaches or security incidents.
- [ ] Check if the plan includes procedures for notifying affected parties.

10) Data Backup and Disaster Recovery

Are data backup and disaster recovery plans implemented?

- [ ] Ensure regular data backups are performed.
- [ ] Verify if there is a disaster recovery plan to restore data in case of an incident.

11) Physical Security

Are physical security measures in place?

- [ ] Check if data centers have controlled access, surveillance, and secure disposal methods for hardware.

12) Compliance Documentation

Is documentation available to demonstrate SOC 2 compliance?

- [ ] Check if the provider can provide compliance reports and certifications.

Ready to ensure your document management system is SOC 2 compliant? Experience the peace of mind that comes with using Docupile.

Wish to secure your files?

Schedule your demo today! Scan Here

4522 Schlipf Rd, Katy, TX, 77493

call: (281) 942-4545

contact@docupile.com

www.docupile.com