Intranet Security & Trust Checklist

It's critical to look for industry-leading security when evaluating intranet providers

When evaluating potential intranet vendors and platforms be sure to take the following security measures into consideration.

It's especially crucial to select an intranet provider that adheres to robust compliance certification by independent auditors — especially if your organization deals with sensitive data or operates in a highly regulated industry like banking or healthcare.

In addition, be careful that your intranet vendor's security isn't self-declared. Look for neutral, third-party assessments from services like BitSight and SecurityScorecard to regularly evaluate intranet security protocols.

			Simpplr	Vendor 2	Vendor 3
Application Vendor	**Vendor has SOC 2 Type 2** Check report shows vendor name		✓		
	Vendor has ISO 27001 Check certificate shows vendor name		✓		
	SLA For system availability		✓ 99.99%		
	Monetary penalty If SLA not met		✓		
Vendor Security Ratings	**Date Scores Retrieved** Rating services update scores frequently		26 September 2023		
	BitSight		800 (Advanced)		
	SecurityScorecard		96 (of 100)		
	Panorays — cyber posture rating		97 (of 100)		
Subprocessors	**Major subprocessors** List the vendor's platform subprocessors		Amazon Web Services (AWS) Salesforce Lightning Platform		
	Subprocessors have SOC 2 Type 2		✓		
	Subprocessors have ISO 27001		✓		
Privacy	**GDPR compliant** Including DPA, SCC, TOSM and DPF		✓		
	CCPA/CPRA compliant California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)		✓		
	TRUSTe Audits DPF compliance and provides dispute resolution		✓		
	Data Privacy Framework (DPF) Including EU-U.S., UK-U.S, and Swiss-U.S. DPF		✓		
Encryption	**Data-at-rest** AES-256 and FIPS 140-2 Level 3 HSM		✓		
	Data-in-transit TLS 1.2 or greater		✓		
Disaster Recovery	**Geographically separate** Primary and secondary servers		✓		
	Near real-time failover		✓		
Automatic Deprovisioning	**SCIM 2.0 support**		✓		

simpplr.com   +1.877.750.8330