SIMPPLR

CHECKLIST

Free intranet security review checklist

FREE INTRANET SECURITY REVIEW CHECKLIST

Keeping your organization's intranet safe requires vigilance — there are always new threats emerging. This checklist is designed as a companion to our step-by-step guide for evaluating and strengthening your intranet's security and compliance. Use this checklist as a comprehensive system check.

Maintaining the checklist

- **Customize** to meet your organization's unique needs.
- **Update** regularly to address evolving security challenges.
- **Engage** stakeholders for a comprehensive and inclusive approach to intranet security.

Tip: Look for industry-leading security when evaluating intranet providers

	Checklist item	Review action	Frequency
User management	**System and application review**	Evaluate all systems and applications tied to the intranet.	Annually
	Role-based access control (RBAC)	Match access limitations to seniority levels, job functions, user roles, etc.	Semi-annually
	User credential standards	Verify that security protocols meet current standards, such as password length and variation.	Quarterly
	Single sign-on (SSO) controls	Assess SSO controls for multiple application access.	Annually
	Account deprovisioning	Check for and deprovision unused staff accounts	Quarterly
Data handling & storage	**Data classification**	Classify data sensitivity and protection requirements as per regulations like GDPR.	Annually
	Data location mapping	Map regulated data locations across the infrastructure.	Semi-annually
	Storage compliance	Confirm that storage aligns with security and compliance prerequisites.	Annually
Coding practices	**Code review**	Review source code of custom applications and integrations using standards like OWASP Top 10 and SANS Top 25.	Annually
	Authentication and access controls	Analyze authentication, input validation, output encoding, etc. to ensure code-level security.	Semi-annually
Data transmission	**Network data review**	Review how data travels through workstations, servers and cloud platforms.	Annually
	Encryption standards	Enable comprehensive encryption to prevent intercepted data during transmissions. Use AES-256 or stronger protections for stored data.	Annually

	Checklist item	Review action	Frequency
Anomaly detection & reporting	**Heuristic analysis**	Implement heuristic analysis for suspicious activities.	Continuous
	Machine learning and AI	Use machine learning and artificial intelligence to find anomalies and attack patterns.	Continuous
	Behavior analysis	Conduct behavior analysis to track irregularities indicative of malware or insider risks.	Continuous
	SIEM & SOC	Review event data capture and correlation to validate enterprise-wide visibility. Examine threat parameters and alerts. Confirm incident-response details like anomaly investigation and threat validation as well as mitigation, recovery and reporting procedures.	Quarterly
Policies, protocols & awareness	**Documentation review**	Review all formal policies and protocols around access controls, acceptable use standards, data ownership, etc.	Annually
	Policy gap analysis	Examine policy gaps discovered in prior breaches to ensure they've been addressed. Ensure policies outline detailed response and recovery processes for security incidents.	Annually
	User awareness	Gauge end-user understanding by surveying staff on core protocols.	Semi-annually
Security & compliance ratings	**Compliance certifications**	Review security and compliance certifications (e.g.,ISO 27001/27002, SOC 2, PCI DSS, GDPR) to ensure they remain active via regular independent audits.	Annually
Performance	**Uptime/Availability**	Assess system/application availability percentages.	Quarterly
	Speed	Review page load times and lag when accessing apps/files.	Semi-annually
	Scalability	Evaluate consistency of performance amid more users, locations and data demands.	Semi-annually
Scalability & growth	**Architecture review**	Review architecture and capacity planning to leave room to smoothly scale amid predictable expansion.	Semi-annually
	Growth planning	Consider upcoming projects (e.g., cloud migrations, new app integrations, intranet modernization) that will require security transitions.	Quarterly
Incident response	**Response protocols**	Review protocols if the intranet is compromised. Initiate sample breach scenarios, then assess the response. Identify successes and areas for improvement.	Annually

FREE INTRANET SECURITY REVIEW CHECKLIST