ENGINEERING SECURITY INSIGHTS

Top 10 PLM Security Checklist

A practical review of foundational controls that help protect engineering data and improve recovery readiness.

How to use this checklist: Review each control with the people responsible for PLM, infrastructure, security, and business continuity. Identify gaps, assign ownership, and prioritize practical improvements.

#	Control	What to evaluate	Why it matters
1	**Strengthen authentication**	Use unique accounts and require MFA for remote or privileged access where practical.	A stolen password alone should not provide easy access to critical systems.
2	**Secure remote access**	Avoid direct Internet exposure of Windchill, Remote Desktop, and administrative interfaces.	Controlled access paths reduce the attack surface and improve accountability.
3	**Maintain patch discipline**	Define ownership and a regular process for operating systems, databases, network devices, and supported components.	Known vulnerabilities remain a common and preventable entry point.
4	**Protect backups**	Maintain separate, offline, or immutable copies of the database, vaults, configuration, and infrastructure dependencies.	Attackers frequently target backups to make recovery more difficult.
5	**Test recovery**	Perform restoration exercises and document the order in which dependent services must be recovered.	A backup is valuable only when the organization can restore a working PLM service.
6	**Apply least privilege**	Review administrators, context teams, groups, service accounts, and inherited permissions.	Excessive access increases the impact of compromised credentials or mistakes.
7	**Monitor infrastructure**	Track CPU, memory, disk, services, patch state, backups, certificates, and security events.	Early visibility can reduce downtime and expose conditions that require attention.
8	**Monitor PLM operations**	Include Method Servers, queues, publishing, Solr, vault capacity, scheduled jobs, and log growth.	Infrastructure can appear healthy while critical PLM functions are degraded.
9	**Secure service accounts**	Use dedicated accounts, limit interactive sign-in, protect credentials, and review ownership.	Service accounts often have broad access and may remain unchanged for long periods.
10	**Maintain an incident plan**	Document contacts, decision authority, isolation steps, recovery priorities, and communication responsibilities.	A prepared response reduces confusion when time and reliable information are limited.

Advisor's Perspective

Security maturity should match the organization's actual risks, resources, and ability to operate the controls it selects. Prioritize improvements that meaningfully reduce exposure and recovery risk today, then reassess as the company and PLM environment evolve.