Security Risk Assessment – Data Breach Incident

Vulnerability	Threat	Impact	Likelihood	Risk Level	Recommendation
Employees share passwords	Unauthorized access to systems by non-authorized personnel	Loss of data integrity, insider threats, privilege escalation	High	High	Enforce unique user credentials and implement password-sharing policy training. Deploy password managers.
Default admin password on database	Brute force or easy unauthorized access to critical systems	Full system compromise, data theft or manipulation	Very High	Critical	Change default passwords immediately. Enforce complex password policies and rotate credentials regularly.
No firewall rules configured	Unrestricted traffic can enter or leave the network	Malware infiltration, data exfiltration, DDoS attacks	High	High	Implement strict inbound/outbound firewall rules. Allow only necessary ports/protocols. Regularly audit firewall configs.
No Multi-Factor Authentication (MFA)	Accounts can be compromised even if passwords are stolen	Account takeovers, privilege abuse, data exposure	High	High	Implement MFA for all critical systems, especially admin and remote access. Use authenticator apps or hardware tokens