GENTOGEN TECHNOLOGIES

Connecting Technology Across Generations

Ghatkopar (E), Mumbai | sales@gentogen.in | gentogen.in

SECURITY HEALTH CHECK – CHECKLIST & REPORT

A practical review of your IT security, data protection and AI-usage readiness

1. Customer & Visit Details

Company		**Report No. / Date**	
Contact person		**Mobile / Email**	
Site / location		**No. of users / PCs**	
Reviewed by	Gentogen Technologies	**Review type**	☐ On-site ☐ Remote

2. What this review covers

We check ten areas against good-practice controls and give you a plain-language report with a short, prioritised action list. The review is based on what we observe and on the information and access you provide on the day. It is a health check, not a certification or a guarantee against attack.

3. Checklist

Mark each item: ✔ OK ✘ Needs action N/A Not applicable

Control / item	Status	Remarks
1. Identity & access		
Multi-factor authentication (MFA) on email, VPN/remote access and admin accounts		
Every user has a unique account; no shared admin or generic logins		
Password policy in place; password manager recommended or used		
Accounts of ex-staff are disabled promptly		
Admin accounts kept separate from daily-use accounts		
2. Laptops & desktops		
Endpoint protection (antivirus/EDR) active and updating on all systems		
Windows and application updates installed regularly		
Disk encryption (e.g. BitLocker) on laptops		
Users do not have local admin rights by default		
USB / removable media usage controlled		
3. Servers & Active Directory		
Servers run supported, patched Windows Server versions		
Stale users, computers and groups cleaned up; Group Policies reviewed		
Privileged groups (Domain Admins etc.) reviewed and minimal		
Remote Desktop (RDP) is not exposed directly to the internet		
Local admin passwords unique per machine (e.g. LAPS)		
4. Network & Wi-Fi		
Firewall rules reviewed; firmware of firewall/router/switches up to date		
No default or weak passwords on network devices		
Wi-Fi uses WPA2/WPA3; guest Wi-Fi isolated from office network		
Remote access via secure VPN with MFA		
Unused ports/services disabled; network diagram available		
5. Email & phishing protection		
SPF, DKIM and DMARC configured for the company domain		
Phishing / spam / malware protection enabled in email platform		
External-sender warnings or similar safeguards enabled		

Staff know how to report a suspicious email		
6. Backup & recovery		
Backups follow 3-2-1 (3 copies, 2 media types, 1 off-site)		
At least one offline or immutable (cannot be changed) copy		
Test restore done in the last 90 days		
Tally and other critical business data included in backup		
Backup failures are monitored and alerted		
7. Data protection		
We know where sensitive data lives (customer, financial, HR data)		
Shared folders and cloud sharing links follow least-access		
Data-loss controls (e.g. sharing restrictions) enabled where available		
Data retention and deletion approach defined		
Basic readiness for India DPDP Act 2023 obligations reviewed (consent, safeguards, breach handling)		
8. AI & cloud app usage		
A written AI usage policy exists and staff have read it		
Only approved, business-grade AI tools are used; no client data in free tools		
Check for unapproved “shadow AI” and cloud apps in use		
Third-party app and vendor access reviewed		
9. Monitoring & incident readiness		
Logs are kept and someone reviews important alerts		
Hardware and software asset inventory is current		
Written steps for “what to do if hacked / ransomware” with contact numbers		
Last incident (if any) was documented and learnt from		
10. People & process		
Staff awareness briefing done in the last 12 months		
Payment or bank-detail changes are verified by a call-back on a known number (guards against fake e-mail and deepfake requests)		
Vendor and contractor access is time-limited and logged		
Server room / network rack physically locked		

GENTOGEN TECHNOLOGIES

Connecting Technology Across Generations

Ghatkopar (E), Mumbai | sales@gentogen.in | gentogen.in

SECURITY HEALTH CHECK – SUMMARY & ACTION PLAN

4. Result summary

Items checked		**Marked OK**	
Needs action		**Not applicable**	
Overall risk level	☐ Low ☐ Medium ☐ High	**Review date**	

Risk level guide: Low – good coverage, minor gaps. Medium – several gaps that attackers commonly use. High – serious gaps (for example no MFA, no tested backup, exposed RDP) that should be fixed first.

5. Priority findings and recommendations

#	Finding	Risk (H/M/L)	Recommendation	Target date
1				
2				
3				
4				
5				
6				
7				

6. Suggested next steps

- Fix the “High” items first (usually MFA, backups, remote-access exposure, patching).
- Adopt the AI usage policy and brief your staff (a template is available from Gentogen).
- Consider an AMC or SLA so that monitoring, patching and backup checks happen regularly.
- Repeat this health check every 6–12 months or after any major change.

7. Limitations

This report reflects the systems, settings and information available at the time of review. It does not include penetration testing or legal advice. No review can guarantee that a security incident will not occur. Legal requirements (such as the DPDP Act) should be confirmed with your legal adviser.

8. Acknowledgement

For GENTOGEN TECHNOLOGIES

Authorized Signatory | Date: _____

Received by CUSTOMER

Name: _____ Signature: _____

Date: _____ (Company stamp)