BlueGuysIT.com
TECHNOLOGY SOLUTIONS

CYBERSECURITY HEALTH CHECKUP SURVEY

Asset Inventory	Address Unauthorized Assets	Software Inventory	Authorized Software Supported	Remove Unauthorized Software	Data Management Process	Data Inventory	Data Access Controls	Data Retention	Secure Data Disposal
Encrypt End-User Devices	Secure Config Process (Assets)	Secure Config Process (Network)	Automatic Session Lock	Firewall on Servers	Firewall on End-User Devices	Manage Assets & Software	Manage Default Accounts	Disable Unnecessary Services	Configure Trusted DNS
Account Inventory	Unique Passwords	Disable Dormant Accounts	Restrict Admin Privileges	Access Granting Process	Access Revoking Process	MFA for External Apps	Vulnerability Management Process	Remediate Based on Risk	Automated OS Patching
Automated App Patching	Log Management Process	Collect Audit Logs	Audit Log Storage	Supported Browsers & Email	DNS Filtering	Anti-Malware Software	Auto Malware Signature Updates	Disable Autorun	Data Recovery Process
Automated Backups	Protect Recovery Data	Isolated Recovery Data	Network Infrastructure Up-to-Date	Secure Config of Network Devices	Remove Unsupported Devices	Awareness Program	Social Engineering Training	Password Policy Training	Data Handling Training
Unintentional Exposure Training	Incident Reporting Training	Update Awareness Training	Insecure Networks Training	Service Provider Inventory	Incident Response Personnel				

Based on the 56 IG1 Safeguards from the globally recognised CIS Controls

SECTION 1: INVENTORY & VISIBILITY

Q1. DO YOU HAVE A COMPLETE INVENTORY OF ALL DEVICES USED IN YOUR BUSINESS?

Answer:

Safeguard 1.1	Establish and Maintain Detailed Enterprise Asset Inventory
Asset Type	Devices
Security Function	Indentify

Plain English: You can’t protect what you don’t know exists. A missing or unmanaged device could be a hole in your defences.

Scoring:

□ All devices are inventoried and reviewed regularly

□ Some devices tracked, but not complete or current

□ No inventory exists or it's outdated

Notes:

Q2. DO YOU HAVE A REGULARLY UPDATED LIST OF ALL SOFTWARE USED IN YOUR BUSINESS?

Answer:

Safeguard 2.1	Inventory and Control of Software Assets
Asset Type	Software
Security Function	Indentify

Plain English: Unapproved or outdated software is a welcome mat for attackers.

Scoring:

□ Accurate list of all licensed software, updated at least twice a year

□ Some tracking done manually or inconsistently

□ No idea what's installed or running

Notes:

SECTION 2: ACCOUNT MANAGEMENT

Q3. ARE USER ACCOUNTS UNIQUE AND PROTECTED BY STRONG PASSWORDS?

Answer:

Safeguard 5.2	Use Unique Passwords
Asset Type	Users
Security Function	Protect

Plain English: Shared or weak passwords are one of the easiest ways for attackers to get in.

Scoring:

□ Every user has a unique, strong password

□ Some shared accounts or reused passwords

□ No password policy or enforcement

Notes:

Q4. ARE OLD, UNUSED USER ACCOUNTS REMOVED WITHIN 45 DAYS?

Answer:

Safeguard 5.3	Disable Dormant Accounts
Asset Type	Users
Security Function	Protect

Plain English: Dormant accounts are often forgotten — until an attacker finds them.

Scoring:

- □ Disabled or deleted after 45 days inactivity
- □ Infrequently reviewed
- □ Left active indefinitely

Notes:

SECTION 2: ACCOUNT MANAGEMENT

Q5. DO YOU RESTRICT ADMIN ACCESS TO DEDICATED ADMIN ACCOUNTS ONLY?

Answer:

Safeguard 5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
Asset Type	Users
Security Function	Protect

Plain English: If everyday users have admin powers, the risk of serious damage skyrockets.

Scoring:

- □ Admin accounts are used only for admin tasks
- □ Admin tasks sometimes done from regular accounts
- □ No admin access restrictions in place

Notes:

SECTION 2: ACCOUNT MANAGEMENT

Q6. DO YOU REQUIRE MULTI-FACTOR AUTHENTICATION (MFA) FOR ALL APPS AND DEVICES?

Answer:

Safeguard 6.3	Require MFA for Externally-Exposed Applications
Asset Type	Users
Security Function	Protect

Plain English: If someone steals your password, MFA is the one thing standing in their way.

Scoring:

□ MFA enforced for all apps

□ MFA used in some places (email, VPN), but not all

□ No MFA in place for remote access

Notes:

SECTION 3: EMPLOYEE AWARENESS

Q7. HAVE EMPLOYEES RECEIVED SECURITY AWARENESS TRAINING IN THE PAST YEAR?

Answer:

Notes:

Safeguard 14.1	Establish and Maintain a Security Awareness Program
Asset Type	Documentation
Security Function	Protect

Plain English: People make mistakes. Phishing, password slips, clicking dodgy links, all of it. Training your team is one of the most effective ways to reduce risk.

Scoring:

□ Everyone trained regularly

□ Some training exists, but not consistent

□ No training done

Notes:

SECTION 3: EMPLOYEE AWARENESS

Q8. ARE EMPLOYEES TRAINED TO REPORT PHISHING AND SUSPICIOUS ACTIVITY?

Answer:

Safeguard 14.2	Train Workforce to Recognize Social Engineering Attacks
Asset Type	Users
Security Function	Protect

Plain English: If employees don't know what to look for, they won't catch it in time.

Scoring:

□ Employees know exactly how and where to report

□ Some informal awareness

□ No reporting system or training

Notes:

SECTION 4: ENDPOINT SECURITY

Q9. IS ANTIVIRUS OR ENDPOINT PROTECTION INSTALLED AND MANAGED ON ALL DEVICES?

Answer:

Safeguard 10.1	Deploy and Maintain Anti-Malware Software
Asset Type	Devices
Security Function	Protect

Plain English: Unprotected devices are an open door for malware and ransomware.

Scoring:

□ All devices protected and centrally managed

□ Some devices covered

□ No consistent AV installed

Notes:

Q10. ARE ALL YOUR DEVICES CONFIGURED TO LOCK AUTOMATICALLY AFTER INACTIVITY?

Answer:

Safeguard 4.3	Configure Automatic Session Locking on Enterprise Assets
Asset Type	Devices
Security Function	Protect

Plain English: Walking away from an unlocked device can be all it takes to get breached.

Scoring:

□ Auto-lock in place for all devices

□ Inconsistent settings

□ No auto-lock configured

Notes:

Q11. DO YOU MANAGE SYSTEMS AND ADMIN ACCESS ONLY THROUGH SECURE, DOCUMENTED METHODS?

Answer:

Safeguard 4.6	Securely Manage Enterprise Assets and Software
Asset Type	Devices
Security Function	Protect

Plain English: Management tools and admin portals should use secure, encrypted access (HTTPS, SSH, VPN with MFA) and follow a documented process.

Scoring:

□ All admin interfaces use secure protocols

□ Mixed usage

□ Insecure protocols still used

Notes:

Q12. IS SENSITIVE DATA ENCRYPTED ON ALL EMPLOYEE DEVICES?

Answer:

Safeguard 3.6	Encrypt Data on End-User Devices
Asset Type	Data
Security Function	Protect

Plain English: If a device gets stolen, encryption keeps your data safe.

Scoring:

□ Full disk encryption on all endpoints

□ Some encryption in place

□ No encryption enabled

Notes:

Q13. DO YOU REGULARLY BACK UP IMPORTANT BUSINESS DATA AND TEST THE BACKUPS?

Answer:

Safeguard 11.1	Establish and Maintain a Data Recovery Process
Asset Type	Documentation
Security Function	Recover

Plain English: If you don't have backups and you're getting a ransomware attack, it's game over.

Scoring:

- □ Backups are automated and tested
- □ Backups exist but rarely tested
- □ No working backup system

Notes:

SECTION 6: WEB & EMAIL THREATS

Q14. DO YOU FILTER OUT KNOWN MALICIOUS WEBSITES AND EMAIL LINKS?

Answer:

Safeguard 9.1/9.2	Ensure Use of Only Fully Supported Browsers and Email Clients & DNS Filtering
Asset Type	Software & Devices
Security Function	Protect

Plain English: Most attacks come through bad links, and you have to stop them at the source.

Scoring:

□ DNS/email filtering in place across all devices

□ Some protections active

□ No filtering

Notes:

Q15. DO YOU HAVE AN INCIDENT RESPONSE PLAN IN CASE OF A CYBERATTACK?

Answer:

Safeguard 17.1	Q15. Do you have an incident response plan in case of a cyberattack?
Asset Type	Users
Security Function	Respond

Plain English: When something goes wrong, someone needs to take charge, not everyone panicking at once.

Scoring:

- □ A responsible person is officially designated and reviewed yearly
- □ It's assumed who's in charge, but not written down or reviewed
- □ No clear person assigned for handling incidents

Notes: