Cyber Security Checklist

v1.0

Item #	Question	Yes	No
Documented Security Procedures & Accountability			
1.	Have you created security policies commensurate with the size and culture of your organisation?	☐	☐
2.	Are security policies documented and updated?	☐	☐
3.	Is maintaining the security of the organisation made part of each employee's job description?	☐	☐
4.	Are all employees required to sign confidentiality agreements?	☐	☐
5.	Are all contractors, facility managers, couriers, maintenance companies, cleaners explicitly informed of the organisations policies and standards that apply to their activities?	☐	☐
6.	Are legal notices posted on log-on and authentication screens warning that unauthorised access or use constitutes an illegal intrusion?	☐	☐
7.	Does the organisation restrict employee access to critical systems and information?	☐	☐
8.	Do you classify your data, identifying sensitive data versus non sensitive?	☐	☐
9.	Are maintenance and cleaning staff prevented from entering areas unsupervised which contain mildly sensitive systems and information and above?	☐	☐
10.	Are employees prohibited from installing personal, or unauthorised software on their organisation supplied computer, laptop, tablet, smart phone or any other device?	☐	☐
11.	Are employees required to have a 'strong' password on personal smart phones and other devices on which they have access to company emails or other sensitive information?	☐	☐
12.	Does the organisations polices define the proper use of email, internet access, instant messaging by employees?	☐	☐
13.	Are employees prohibited from sharing passwords and allowing other employees to use their computers and portable devices?	☐	☐
14.	Are there procedures in place to prevent computers from being left in a logged-on state, however briefly?	☐	☐
15.	Is the employee who is responsible for a given piece of information equipment required to oversee the security of that equipment?	☐	☐
16.	Is each piece of equipment tagged using a permanent identifier and or the serial number recorded to determine who is entrusted with the piece of equipment?	☐	☐
17.	Are there measures to prevent employees from leaving the business premises with sensitive information carried on USB or other media devices?	☐	☐
18.	Are employees provided sufficient incentives to report security breaches and improper security practices and at the same time protected from retribution or blame from making such a report?	☐	☐
19.	Is there a procedure in place to immediately revoke all passwords and/or prevent access to company property, data intellectual property, customer records, restricted physical areas and to any supplier or customer of the organisation?	☐	☐
20.	Are employees prohibited from allowing other staff or any other person to use their swipe card, keys, pin numbers and the like to gain access of information facilities or systems?	☐	☐
Backup Procedures & Security			
21.	Are the operating systems, programs and operating information backed up as well as the data/records?	☐	☐

22.	Is the data being backed up at a frequency appropriate to its sensitivity and importance to the organisation?	☐	☐
23.	Does the back-up procedure include checking the data for hostile code such as Trojan horses or viruses?	☐	☐
24.	If the information being backed up is proprietary or sensitive, is the information encrypted and stored as such during the back-up process?	☐	☐
25.	Are all copies of back-ups protected from loss by fire, theft and accidental damage?	☐	☐
26.	When storage media is no longer required are there secure procedures for destroying or reusing the media?	☐	☐
27.	Are there multiple backups so that if one is lost or corrupted, the system could still be restored?	☐	☐
28.	Are the backups being retained long enough so that there would still be an uncorrupted copy if the data was gradually being corrupted or the system was shut down as part of a ransom or other malicious attack?	☐	☐
29.	Are all relevant logs of activity backed up and securely stored to prevent alteration?	☐	☐
30.	Are the configurations of switches and routers backed up on a regular basis?	☐	☐
31.	Are the backups regularly stored at a physically remote location?	☐	☐
32.	Are the backups regularly tested to ensure they are working as they should?	☐	☐
33.	Are there procedures to deal with the loss or theft of unencrypted backup data that is proprietary or of a sensitive nature?	☐	☐
Security of Hardware, Data & Records			
34.	Is all electronic equipment (hardware and software) listed on an accurate inventory listing and where appropriate housed in a secure area?	☐	☐
35.	Are there documented, quick and easy, procedures for updating the inventory whenever it is to be moved or the person allocated to use/protect it changes?	☐	☐
36.	Is each piece of equipment labelled with a bar code or other identifier for easy tracking?	☐	☐
37.	Is there a procedure for the removal and destruction of hard discs or other media when the equipment reaches the end of its useful life or is otherwise taken out of service permanently?	☐	☐
38.	Do you have procedures for disposing of waste material?	☐	☐
39.	Where equipment is being reassigned to a different employee, is there a procedure in place to ensure that sensitive information is not left on the machine that would not normally be accessible by the employee entrusted with the equipment moving forward?	☐	☐
40.	Are there periodic checks to ensure that the equipment is where it is reported to be?	☐	☐
41.	Do you have policies covering laptop security (e.g. cable lock or secure storage)?	☐	☐
42.	Are especially important items of electronic equipment housed in a secure datacenter, room or cabinet?	☐	☐
43.	Are their physical barriers of access to the equipment commensurate to the value of the equipment and the data contained on it?	☐	☐
44.	Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?	☐	☐
45.	Are there clear and rigorously enforced restrictions on who has access to the datacenter, computer room or cabinets?	☐	☐
46.	Do your policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?	☐	☐
47.	Are there strict policies outlining the procedures for afterhours access to the datacenter, or computer room by personnel such as custodians?	☐	☐

48.	Does the datacenter or main computer room have a sign-in procedure that is used to record non-employees into the restricted space?	☐	☐
49.	Are data centres, data rooms and data cabinets protected by adequate fire and burglary detectors and or CCTV and or fire suppression systems commensurate with the cost of the loss of the equipment, data or records?	☐	☐
50.	Is there sufficient heating and cooling to the datacenter/computer room to maintain a consistent safe operating temperature for the electronic equipment?	☐	☐
51.	Is the electronic equipment protected from moisture or excessive humidity, dust, smoke, chemical fumes or other potentially damaging substances?	☐	☐
52.	Is there a risk of water entry to any area housing critical equipment or records from water pipes, hot water systems, waste pipes, storm water pipes, box gutters or sprinkler systems?	☐	☐
53.	Is physical access to the console interfaces of security systems such as those used to manage firewalls, CCTV and intrusion systems, restricted to authorised users?	☐	☐
54.	Do you ensure users have anti-virus software loaded and active on systems?	☐	☐
55.	Are documents that contain sensitive information secured or otherwise protected from unauthorised printing?	☐	☐
56.	Does the company have a documented and enforced procedure for the safe disposal of paper records that are no longer required?	☐	☐
57.	Is waste paper binned or shredded?	☐	☐
58.	Are there sufficiently rigorous policies and procedures governing the use of removable magnetic media, such as USB devices?	☐	☐
59.	Are there sufficiently rigorous procedures to restrict unauthorised access to back-up media?	☐	☐
Power Supply			
60.	Are all important pieces of equipment protected with surge protectors and uninterruptable power supplies?	☐	☐
61.	Are electrical supply components, such as fuse boxes, protected from unauthorized access?	☐	☐
62.	If the systems are sufficiently critical to the organisation, are they connected to a dual source of electricity?	☐	☐
63.	Is there an adequate back-up generator, protected with security devices such as locks alarms and if located outside a building, fences and barbed wire?	☐	☐
64.	Does any back-up generator have ample fuel for a reasonably lengthy power outage, at least long enough to source further supplies?	☐	☐
65.	Does the back-up generator have an automatic switch over when the power goes off and back the other way when the public supply is returned?	☐	☐
Security of Access Ports & Communication Lines			
66.	Are unused network or telecommunication access points physically disabled to prevent unauthorised access?	☐	☐
67.	Where the network and telecommunications ports are not disabled are there procedures to monitor for unauthorised access to these ports?	☐	☐
68.	Are there physical barriers to protect the network cables running to and from the equipment to reduce accidental or deliberate damage?	☐	☐
Training on Security Procedures			
69.	Are all staff provided with periodic training on the organisations security policies with explanation as to why the policies are important and compliance will be enforced?	☐	☐
70.	Are employees trained/warned on the importance of keeping watch and or securing laptops and other portable information devices when taking them outside the workplace?	☐	☐
71.	Are employees trained to use ‘strong’ passwords and not to base passwords on biographical details that may be publically available?	☐	☐

72.	Are employees trained not to store passwords in insecure places such as their wallet, purse, or post-it-note on their computer?	☐	☐
73.	Are employees trained/reminded of what type of information handled by the organisation should be regarded as sensitive information?	☐	☐
74.	Are employees trained/reminded to save sensitive/critical data to a server where it's being backed up?	☐	☐
75.	Are employees trained to be suspicious of any software that arrives in the mail, even where it appears to be packaged by a trusted vendor?	☐	☐
76.	Are employees regularly trained not to download executable code, not to open suspect emails, and not to install personal software on computer systems?	☐	☐
77.	Are employees trained not to visit illicit websites including file sharing/downloading websites?	☐	☐
78.	Are your employees able to identify and protect classified data, including paper documents, removable media, and electronic documents?	☐	☐
79.	Are employees trained on the risk created by installing network links that are undocumented and not authorised even when the link may be requested by a senior manager?	☐	☐
80.	Are employees and contractors prevented from accessing file that would advise when their behaviour is being monitored or attracted special attention?	☐	☐
Incident Handling and Response			
81.	Do staff know how, when and where to report a breach of company policy and or a possible cyber-attack?	☐	☐
82.	Do employees know how to isolate and quarantine compromised systems by removing them from the network?	☐	☐
Internal Policies for Software Development			
83.	Does the organisation have a written policy detailing the steps and procedures for the internal development of software?	☐	☐
84.	Does the software development cycle follow guidelines based on industry best practices concerning security?	☐	☐
85.	Do corporate security policies require all vendor and contractor personnel working on software development to meet minimum security requirements?	☐	☐
86.	Does the organisation have a system for tracking exactly which employee or outside contributor wrote each line of code for any software produced internally?	☐	☐
87.	Are commentaries maintained on each section code as it is being written, so that other developers and security specialists can rapidly understand what a given section is designed to do?	☐	☐
Security Features/ Testing of New Software			
88.	Is the application being developed designed to encrypt sensitive information that it stores in a file or database or local system registry?	☐	☐
89.	Is the software that the organisation has developed subjected to a code review from a security standpoint, regardless of whether it was outsourced or produced in-house, before the final version is readied for deployment?	☐	☐
90.	Does the organisation have information security professionals conduct vulnerability tests of the software it has developed, regardless of whether it was outsourced or produced in-house?	☐	☐
91.	Does the organisation have information security specialists conduct regular vulnerability testing against applications as they are deployed?	☐	☐
Establishing Appropriate Relationships with Vendors			
92.	Do organisational policies require vendor personnel to sign non-disclosure agreements?	☐	☐
93.	Are software vendors required to certify that their code has undergone a rigorous and thorough security inspection before it is delivered for deployment?	☐	☐

94.	When software updates need to be applied, is there a guarantee that those updates were adequately tested in the relevant kind of software environment before being installed?	☐	☐
95.	Are there provisions to maintain the system‘s performance during the update process and to restore the system to its last known good state if an update fails?	☐	☐
96.	Do you ensure users have anti-virus software loaded and active on systems?	☐	☐
97.	Do employees know where and to whom they can go to obtain additional information and guidance on the recovery process?	☐	☐

Ref: Manning, A., & Manning, S. A. (2014). *Mannings Guide to Cyber Security & Insurance*. (LMIGroup, Ed.). Melbourne. Retrieved from http://lmigroup.com/content.aspx?artId=542&catId=26