Cybersecurity Checklist

This document is a checklist designed to identify and document the existence (or lack of) a basic set of cybersecurity policies, procedures, and standards. Check each list item against your organization's current status, but for list items that do not apply to your organization, simply leave that item blank. If you are not sure of the answer, assume it is "No" just to be safe.

Personnel	Yes	No
1. Does your staff wear photo ID badges?	☐	☐
2. Do you have clearly labeled "Guest" badges for visitors and contractors?	☐	☐
3. Do you have a process for screening and vetting contractors?	☐	☐
4. Do you have a clear policy for terminating access to facilities or data for departing employees or contractors?	☐	☐

Physical / Premises Security	Yes	No
1. Is your workplace protected by entry controls, video surveillance, and alarm systems?	☐	☐
2. Do you have policies and procedures in place to control access to areas where private data is housed (server rooms, etc.)?	☐	☐
3. Is there a single point of entry for visitors and contractors?	☐	☐
4. Are there policies in place governing how visitors and contractors are logged (sign-in/out, electronic scheduling, etc.)?	☐	☐
5. Are visitors escorted in and out of controlled areas?	☐	☐
6. Is your guest Wi-Fi network connected to your private work network?	☐	☐
7. Are your staff's workspaces restricted from public access?	☐	☐
8. Are there any access points to your network (workstations, etc.) that are in public areas or areas outside of surveillance?	☐	☐
9. Are there policies in place dictating when a user is auto-logged out of a workstation and when a screen shuts off after a period of inactivity?	☐	☐
10. Do you have procedures for protecting data during equipment repairs?	☐	☐
11. Are portable assets (laptops, tablets, etc.) physically secured when not in use?	☐	☐
12. Do you have a current emergency evacuation plan?	☐	☐
13. Do you have a plan to identify areas that need to be sealed off immediately in case of an emergency?	☐	☐
14. Have you drilled your emergency plans within the past 12 months?	☐	☐

Cybersecurity Checklist

Compliance and Auditing

	Yes	No
1. Do you have policies covering electronic authentication, authorization, and access control for your information systems, applications, and data?	☐	☐
2. Do you enforce password strength standards (not easy to guess, not generic, numbers and symbols, etc.)?	☐	☐
3. Do you enforce regular password changes for your workstations and apps (once a month, once a quarter, etc.)?	☐	☐

Data Security

	Yes	No
1. Do you classify your data into “sensitive” and “non-sensitive?”	☐	☐
2. Do you have policies in place to restrict access to data by unauthorized persons?	☐	☐
3. Do you encrypt valuable or sensitive information?	☐	☐
4. Do you have procedures covering the management of private personal information?	☐	☐
5. Is there a process in place to securely replicate and store copies of important data?	☐	☐
6. Do you have clear policies in place governing the destruction of digital data (data shredding apps, etc.)?	☐	☐
7. Do you have clear policies in place governing the destruction of physical data (old hard drives, paper documents, tapes, CDs, etc.)?	☐	☐
8. Is the waste from the destruction of physical data assets handled by trusted professionals?	☐	☐

Staff Security Awareness and Education

	Yes	No
1. Do you hold staff training for computer and data security?	☐	☐
2. Is your security training regular (once a quarter, once a year, etc.)?	☐	☐
3. Are employees trained to spot network intrusion and scam attempts?	☐	☐
4. Is there a clear policy for reporting network intrusion and scam attempts?	☐	☐
5. Are employees trained to appropriately identify sensitive data and assets (cloud folders, paper documents, removable media, etc.)?	☐	☐

Cybersecurity Checklist

Staff Security Awareness and Education	Yes	No
1. Do you hold staff training for computer and data security?	☐	☐
2. Is your security training regular (once a quarter, once a year, etc.)?	☐	☐
3. Are employees trained to spot network intrusion and scam attempts?	☐	☐
4. Is there a clear policy for reporting network intrusion and scam attempts?	☐	☐
5. Are employees trained to appropriately identify sensitive data and assets (cloud folders, paper documents, removable media, etc.)?	☐	☐

Response Analysis

For each question that is marked “No,” carefully review its impact and relevance to your organization. Consider implementing or updating policy to address any relevant issues. If several questions that are relevant to your organization are marked “No,” consider a restructuring of your security posture.

REMINDER: This checklist is designed to give you a **BASIC** overview of your security posture. Leveraging a professional cybersecurity consultant will help you get a more detailed overview of your security status and provide clear and actionable recommendations for remediation of any vulnerabilities.