# **A blue background with white lines AI-generated content may be incorrect.**

# **Cyber Security: Best Practices for U.S. Based Businesses + Checklist**

This Cyber Security Best Practices for U.S. Based Businesses guide outlines essential cybersecurity practices for protecting sensitive business information, infrastructure, and data from cyber threats. All employees and departments should adhere to these guidelines to minimize risks and ensure compliance with industry standards.

## 1. Network Security

* **Firewalls and Network Segmentation:**
  + Ensure that firewalls are enabled and properly configured on all networks.
  + Implement network segmentation to limit access to sensitive data and systems.
* **Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS):**
  + Deploy IDS/IPS to monitor and block potential security threats on the network.
* **Secure Wi-Fi Networks:**
  + Use strong passwords and WPA3 encryption for all Wi-Fi networks.
  + Limit access to authorized users only.
* **Virtual Private Network (VPN) for Remote Workers:**
  + Require the use of a secure VPN for all employees working remotely to access company resources.

## 2. Endpoint Security

* **Antivirus and Anti-Malware Protection:**
  + Ensure all devices (desktops, laptops, mobile devices) are equipped with up-to-date antivirus and anti-malware software.
* **Patch Management:**
  + Regularly update software, operating systems, and applications to address known vulnerabilities.
  + Automate patching whenever possible to ensure timely updates.
* **Device Encryption:**
  + Encrypt sensitive data on all devices, including laptops, mobile phones, and USB drives.
* **Mobile Device Management (MDM):**
  + Implement MDM to control and secure mobile devices used for work purposes.

## 3. Access Control

* **Least Privilege Principle:**
  + Grant employees access only to the information and systems necessary for their job function.
* **Multi-Factor Authentication (MFA):**
  + Implement MFA for access to all sensitive systems and applications, including email, file sharing, and cloud platforms.
* **Strong Password Policies:**
  + Enforce strong password requirements (e.g., minimum length, complexity, and regular changes).
  + Use a password manager to store and generate secure passwords.
* **Account Lockout Policies:**
  + Set account lockout policies after a defined number of failed login attempts to prevent brute force attacks.
* **Role-Based Access Control (RBAC):**
  + Use RBAC to restrict access to sensitive data and systems based on employees' roles and responsibilities.

## **4. Data Security and Backup**

* **Data Classification:**
  + Classify company data into categories (public, internal, confidential, etc.) and apply appropriate security measures based on the classification.
* **Regular Data Backups:**
  + Schedule and automate regular backups of critical data and systems.
  + Store backups in a secure, off-site location or cloud-based solution.
  + Test backup recovery processes to ensure they work in case of a data breach or ransomware attack.
* **Data Retention and Disposal:**
  + Implement a data retention policy and securely dispose of unnecessary or outdated data.
  + Ensure that sensitive data is properly wiped from devices before disposal.

## 5. Email and Communication Security

* **Email Filtering and Anti-Phishing Measures:**
  + Use email filters to block malicious emails, spam, and phishing attempts.
  + Provide employees with regular phishing awareness training and conduct simulated phishing tests.
* **Encrypted Email:**
  + Use email encryption for sending sensitive information over email.
* **Secure File Sharing:**
  + Encourage the use of secure, company-approved file sharing platforms instead of personal email or third-party tools.

## 6. Security Awareness Training

* **Employee Cybersecurity Training:**
  + Provide ongoing cybersecurity awareness training to all employees, focusing on phishing, password security, social engineering, and data protection best practices.
* **Cybersecurity Policies and Procedures:**
  + Ensure all employees are aware of and follow your company’s cybersecurity policies, including reporting security incidents and adhering to data protection guidelines.
* **Incident Response Training:**
  + Train employees to identify and report security incidents, such as suspicious emails or unauthorized system access, following established protocols.

## 7. Incident Response and Disaster Recovery

* **Incident Response Plan (IRP):**
  + Develop and maintain an IRP that outlines the steps to take in the event of a cybersecurity breach.
  + Conduct regular mock drills to test the effectiveness of the plan.
* **Disaster Recovery Plan (DRP):**
  + Develop and test a DRP to ensure business continuity in the event of a cyberattack or system failure.
  + Ensure that critical business operations can be resumed within an acceptable time frame.

## 8. Vendor and Third-Party Risk Management

* **Vendor Security Assessments:**
  + Perform regular security assessments of third-party vendors to ensure they comply with your company's security requirements.
* **Third-Party Access Controls:**
  + Limit third-party access to your network and data, and enforce security protocols for any third-party services.
* **Contractual Agreements:**
  + Include cybersecurity clauses in vendor contracts to ensure they adhere to required security measures and breach notification procedures.

## 9. Compliance with Regulations

* **Compliance with Federal and State Regulations:**
  + Ensure adherence to cybersecurity regulations, such as **CMMC (Cybersecurity Maturity Model Certification)**, **GDPR**, **CCPA**, **HIPAA**, and other relevant local, state, or industry-specific laws.
* **Data Breach Notification:**
  + Establish a protocol for notifying stakeholders and authorities of data breaches, in compliance with data protection laws.

## 10. Continuous Monitoring and Improvement

* **Regular Security Audits:**
  + Perform periodic security audits and vulnerability assessments to identify and mitigate potential risks.
* **Penetration Testing:**
  + Conduct regular penetration tests to identify weaknesses and ensure systems can withstand cyberattacks.
* **Threat Intelligence:**
  + Subscribe to threat intelligence feeds to stay informed about the latest cyber threats and vulnerabilities.

## Conclusion

Cybersecurity is a critical aspect of maintaining the integrity of your company’s operations and protecting sensitive information. By following these best practices, you ensure that your company is well-prepared to prevent and respond to cyber threats. Regularly reviewing and updating security policies and procedures is essential to staying ahead of evolving risks.

This checklist can be customized to fit your specific business and operational needs. Regular reviews and updates should be conducted to ensure that your business remains compliant with the latest security standards.

## **Cybersecurity Internal Checklist:**

| **Category** | **Best Practice** | **Action Required** | **Responsible Party** | **Date Completed** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| **Network Security** | Firewalls and Network Segmentation | Ensure firewalls are enabled and configured for all networks | IT Department |  |  |
|  | Intrusion Detection and Prevention Systems (IDS/IPS) | Deploy IDS/IPS to monitor and block potential threats | IT Department |  |  |
|  | Secure Wi-Fi Networks | Use WPA3 encryption and strong passwords for Wi-Fi networks | IT Department |  |  |
|  | Virtual Private Network (VPN) for Remote Workers | Require secure VPN for remote work access | IT Department |  |  |
| **Endpoint Security** | Antivirus and Anti-Malware Protection | Install and update antivirus software on all devices | IT Department |  |  |
|  | Patch Management | Regularly update software, OS, and applications to address vulnerabilities | IT Department |  |  |
|  | Device Encryption | Encrypt sensitive data on all devices | IT Department |  |  |
|  | Mobile Device Management (MDM) | Implement MDM for control of mobile devices | IT Department |  |  |
| **Access Control** | Least Privilege Principle | Grant employees access to necessary data only | HR/IT Department |  |  |
|  | Multi-Factor Authentication (MFA) | Implement MFA for sensitive systems and applications | IT Department |  |  |
|  | Strong Password Policies | Enforce strong password policies and use password managers | HR/IT Department |  |  |
|  | Account Lockout Policies | Set policies for failed login attempts | IT Department |  |  |
|  | Role-Based Access Control (RBAC) | Restrict access to sensitive data based on roles | IT Department |  |  |
| **Data Security and Backup** | Data Classification | Classify data and apply appropriate security measures | IT Department |  |  |
|  | Regular Data Backups | Automate and store backups securely; test recovery | IT Department |  |  |
|  | Data Retention and Disposal | Implement data retention policy and securely dispose of data | IT/HR Department |  |  |
| **Email and Communication Security** | Email Filtering and Anti-Phishing Measures | Use filters and provide phishing awareness training | IT Department |  |  |
|  | Encrypted Email | Use encryption for sensitive emails | IT Department |  |  |
|  | Secure File Sharing | Use company-approved file-sharing platforms | Employees |  |  |
| **Security Awareness Training** | Employee Cybersecurity Training | Provide ongoing training on phishing, password security, etc. | HR/IT Department |  |  |
|  | Cybersecurity Policies and Procedures | Ensure all employees are aware of security policies | HR Department |  |  |
|  | Incident Response Training | Train employees to identify and report incidents | HR/IT Department |  |  |
| **Incident Response and Disaster Recovery** | Incident Response Plan (IRP) | Develop and test incident response plan | IT Department |  |  |
|  | Disaster Recovery Plan (DRP) | Develop and test disaster recovery plan | IT Department |  |  |
| **Vendor and Third-Party Risk Management** | Vendor Security Assessments | Regularly assess vendor security | Procurement/IT Department |  |  |
|  | Third-Party Access Controls | Limit third-party access to sensitive data | IT Department |  |  |
|  | Contractual Agreements | Include cybersecurity clauses in contracts | Legal/Procurement Department |  |  |
| **Compliance with Regulations** | Compliance with Federal and State Regulations | Ensure compliance with CMMC, HIPAA, GDPR, etc. | Legal/Compliance Department |  |  |
|  | Data Breach Notification | Establish protocols for notifying authorities in case of a breach | IT/Legal Department |  |  |
| **Continuous Monitoring and Improvement** | Regular Security Audits | Perform periodic security audits | IT Department |  |  |
|  | Penetration Testing | Conduct regular penetration tests to identify vulnerabilities | IT Department |  |  |
|  | Threat Intelligence | Subscribe to threat intelligence feeds and stay informed on risks | IT Department |  |  |

**How to Use the Spreadsheet:**

1. **Category:** The cybersecurity area being addressed.
2. **Best Practice:** The specific security measure or action to be taken.
3. **Action Required:** Details on the specific steps or actions needed to implement the best practice.
4. **Responsible Party:** The department or person responsible for carrying out the action.
5. **Date Completed:** The date the task was completed (helps with tracking and compliance).
6. **Notes:** Additional comments or reminders for context.

You can copy this table into a spreadsheet tool (e.g., Google Sheets or Microsoft Excel). This will allow you to track the progress of cybersecurity initiatives and maintain records of security activities over time. If you're using a tool like Google Sheets, you can also set up conditional formatting, alerts, or reminders for actions that need attention.

**A blue background with white lines

AI-generated content may be incorrect.**