

# Safeguarding Taxpayer Data Checklist

| Category                      | Details                                                                                                                                    | Status                   |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Background checks             | Check references or conduct background checks before hiring employees who will have access to customer information.                        | <input type="checkbox"/> |
| Confidentiality agreements    | Ask new employees to sign an agreement to follow your company's security standards for handling customer information.                      | <input type="checkbox"/> |
| Limit information access      | Limit access to customer information to employees who have a business reason to see it.                                                    | <input type="checkbox"/> |
| Strong passwords              | Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis.          | <input type="checkbox"/> |
| Multi-factor authentication   | Require multi-factor authentication for anyone accessing customer information on your system.                                              | <input type="checkbox"/> |
| Lock computers                | Use password-activated screen savers to lock employee computers after a period of inactivity.                                              | <input type="checkbox"/> |
| Device protection             | Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices.                                | <input type="checkbox"/> |
| Basic security steps          | Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information.                      | <input type="checkbox"/> |
| Encrypt sensitive information | Encrypt sensitive customer information when it is transmitted electronically via public networks.                                          | <input type="checkbox"/> |
| Designate trained individuals | Refer calls or requests for customer information to individuals who have been trained in how your company safeguards personal data.        | <input type="checkbox"/> |
| Report suspicious attempts    | Report suspicious attempts to obtain customer information to designated personnel.                                                         | <input type="checkbox"/> |
| Regular reminders             | Regularly remind all employees of your company's policy to keep customer information secure and confidential.                              | <input type="checkbox"/> |
| Remote work policies          | Develop policies for employees who telecommute.                                                                                            | <input type="checkbox"/> |
| Security policy violations    | Impose disciplinary measures for security policy violations.                                                                               | <input type="checkbox"/> |
| Access deactivation           | Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names.               | <input type="checkbox"/> |
| Label important documents     | Add labels to documents to signify importance, such as "Sensitive" or "For Official Business" to further secure paper documents.           | <input type="checkbox"/> |
| Secure storage                | Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access.                | <input type="checkbox"/> |
| Computer inventory            | Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.              | <input type="checkbox"/> |
| Secure data transmission      | Take steps to ensure the secure transmission of customer information.                                                                      | <input type="checkbox"/> |
| Secure disposal               | Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule.                            | <input type="checkbox"/> |
| Monitor for threats           | Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and defenses.        | <input type="checkbox"/> |
| Maintain software             | Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information.                          | <input type="checkbox"/> |
| Up-to-date firewalls          | Maintain up-to-date firewalls on computers and office networks.                                                                            | <input type="checkbox"/> |
| Close unused ports            | Regularly ensure that ports not used for your business are closed.                                                                         | <input type="checkbox"/> |
| Security information          | Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.                       | <input type="checkbox"/> |
| Monitor network activity      | Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information.                           | <input type="checkbox"/> |
| Detect attacks                | Use an up-to-date intrusion detection system to alert you of attacks.                                                                      | <input type="checkbox"/> |
| Monitor data transfers        | Monitor both in- and out-bound transfers of information for indications of a compromise.                                                   | <input type="checkbox"/> |
| Insert dummy accounts         | Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.            | <input type="checkbox"/> |
| Secure compromised data       | Take immediate action to secure any information that has or may have been compromised.                                                     | <input type="checkbox"/> |
| Review breach evidence        | Preserve and review files or programs that may reveal how the breach occurred.                                                             | <input type="checkbox"/> |
| Professional assessment       | If feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.                                | <input type="checkbox"/> |
| Notify stakeholders           | Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach.                                        | <input type="checkbox"/> |
| Data loss response            | Practitioners who experience a data loss should contact the IRS and the states, and consider having a technical support contract in place. | <input type="checkbox"/> |