Small Business IT Risk Assessment

Company name:			
Completed by:		Date:	

Where Do I Begin?
A risk assessment is an important step in protecting your customers, employees, and your business, and well as complying with the law. This Information Technology Risk Assessment survey helps identity all of the information assets you handle, the controls in place, and areas of high risk or threats. Steps for completing this risk assessment:

Step 1: Complete the questionnaire below. Use additional paper as needed to add notes or new survey questions.

Step 2: Based on your responses apply a risk rating for each of the applicable categories.
Rate your risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure.

Step 3: List specific areas of high risk or threats, along with any new control that may be needed

Step 4: Present your findings to management and the board, and implement new controls as needed.

Step 5: Update your risk assessment at least once a year, comparing your results to previous versions

I. Company Information			
Business primary address:			
Phone:		Date company was formed:	
Number of employees (FTE):			
Type of business (check one):	☐Corporation ☐Partnership ☐Individual ☐Other_____		
Nature of business:			
Website url(s):			
Do you conduct business outside the US?	☐Yes ☐No	If yes, identify countries:	

II. Management Supervision	
Management and board supervision are essential for an effective information security program, and often mandated by state and federal regulations.	
Do you have a written information security plan?	☐Yes ☐No ☐N/A
Are you aware of, and in compliance with, any laws mandating information security?	☐Yes ☐No ☐N/A
Are adequate data protection procedures in place and monitored by management?	☐Yes ☐No ☐N/A
Do you use third party vendors for managing your network?	☐Yes ☐No ☐N/A
Do third party vendor contracts provide adequate controls?	☐Yes ☐No ☐N/A
Are third party contracts monitored at least annually?	☐Yes ☐No ☐N/A
Are sufficient procedures in place for incident reporting?	☐Yes ☐No ☐N/A
Do you have a business continuity plan and/or disaster recovery plan?	☐Yes ☐No ☐N/A
Do you deliver up-to-date security training to management and staff?	☐Yes ☐No ☐N/A
Is the Board actively involved with your information security plans and procedures?	☐Yes ☐No ☐N/A

Rate your Management Supervision risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:							
Least Secure	☐1	☐2	☐3	☐4	☐5	Most Secure	
Reason for the rating:							

List areas of high risk (threats):	List new controls needed:

III. Personnel Security

Pre-employment screening, such as background checks, should be conducted for individuals that will handle sensitive information.

Do you perform background checks on all employees with access to sensitive information?	☐Yes ☐No ☐N/A
Do background checks include criminal history?	☐Yes ☐No ☐N/A
Are photo IDs required for employment?	☐Yes ☐No ☐N/A
Are photo IDs or visitor badges worn in the workplace?	☐Yes ☐No ☐N/A
Do you delete security access immediately upon employee termination?	☐Yes ☐No ☐N/A

Rate your Personnel Security risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:							
Least Secure	☐1	☐2	☐3	☐4	☐5	Most Secure	
Reason for the rating:							

List areas of high risk (threats):	List new controls needed:

IV. Physical Security	
This section helps identity the physical security controls in place, and determine if any physical weaknesses exist for protecting sensitive information	
Is access to the building(s) securely maintained during business hours and after hours?	☐Yes ☐No ☐N/A
Are sufficient locks maintained on all doors, windows, and entrances?	☐Yes ☐No ☐N/A
Do you have a security alarm system?	☐Yes ☐No ☐N/A
Do you have security cameras on premise?	☐Yes ☐No ☐N/A
Are employees and/or visitors required to wear badges?	☐Yes ☐No ☐N/A
Is the building(s) adequately protected against fire?	☐Yes ☐No ☐N/A
Does the building(s) have a fire alarm system?	☐Yes ☐No ☐N/A
Is the building(s) protected with sprinklers?	☐Yes ☐No ☐N/A
Are sensitive files and documents stored in fireproof files or vaults?	☐Yes ☐No ☐N/A
Is the building(s) adequately protected against water damage?	☐Yes ☐No ☐N/A
Is access to network equipment such as servers and storage media containing sensitive data physically protected? (Check all that apply)	☐Yes ☐No ☐N/A
☐ Areas are restricted to authorized employees only	☐ Software permission controls
List other physical security issues for your business:	

Rate your Physical Security risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:							
Least Secure	☐1	☐2	☐3	☐4	☐5	Most Secure	
Reason for the rating:							

List areas of high risk (threats):	List new controls needed:

V. Identify Your Information Assets	
Using the list of common types of information assets below, identify all types of consumer, employee and business information that your company handles. Mark the level of risk (Low, Medium, or High) for each item, or N/A if it is not applicable to your business. Use the following risk level descriptions as a guideline:	
Level 1: Low Risk	Information you handle for customers, personnel, and your business that is publicly available.
Level 2: Medium Risk	This level of information generally includes information that is not Personally Identifiable Information (PII), or information that would not harm your customers, employees, or your business such as, phone numbers, office policies, vendor information, etc.
Level 3: High Risk	Highly sensitive information your business handles or has access to such as customer records, personnel files, credit/debit card numbers or other payment information, financial reports, passwords, PIN, social security numbers, etc. *Note: If this type of information is used by your company and is present on websites, computer systems, mobile devices or emails, it must be rated as Level 3: High Risk.*

Customer and Employee Information	Level of Risk
Individual addresses/phone numbers	☐1-Low ☐2-Medium ☐3-High ☐N/A
Email addresses	☐1-Low ☐2-Medium ☐3-High ☐N/A
Date of birth	☐1-Low ☐2-Medium ☐3-High ☐N/A
SSN	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
Password/PIN	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
Photos/signatures	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
Account information	☐1-Low ☐2-Medium ☐3-High ☐N/A
Purchase/transaction history	☐1-Low ☐2-Medium ☐3-High ☐N/A
Criminal history	☐1-Low ☐2-Medium ☐3-High ☐N/A
Employee records	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
Medical records	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
Financial/banking	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
Legal documents	☐1-Low ☐2-Medium ☐3-High ☐N/A
Credit/debit card information	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
ACH/electronic payments	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
Paper checks	☐1-Low ☐2-Medium ☐**3-High** ☐N/A
List other highly sensitive customer/employee information:	

Business Information	Level of Risk
Public information/brochures	☐1-Low ☐2-Medium ☐3-High ☐N/A
Press releases	☐1-Low ☐2-Medium ☐3-High ☐N/A
Social media postings	☐1-Low ☐2-Medium ☐3-High ☐N/A
Office policies	☐1-Low ☐2-Medium ☐3-High ☐N/A
Vendor information	☐1-Low ☐2-Medium ☐3-High ☐N/A

Management/board member credentials	☐1-Low	☐2-Medium	☐3-High	☐N/A
Management/board reports	☐1-Low	☐2-Medium	☐3-High	☐N/A
Email correspondence	☐1-Low	☐2-Medium	☐3-High	☐N/A
Purchase orders	☐1-Low	☐2-Medium	☐3-High	☐N/A
Accounting/financial	☐1-Low	☐2-Medium	☐3-High	☐N/A
Marketing/sales	☐1-Low	☐2-Medium	☐3-High	☐N/A
Legal/contracts	☐1-Low	☐2-Medium	☐3-High	☐N/A
Medical/insurance records	☐1-Low	☐2-Medium	☐3-High	☐N/A
Trade secrets/patents	☐1-Low	☐2-Medium	☐3-High	☐N/A
List other highly confidential information that is the lifeblood of a company:				

Public-Facing Website	**Level of Risk**			
Identify and rate all information you collect and/or share with customers via a Website?				
Personal information (names, address, phone, etc.)	☐1-Low	☐2-Medium	☐3-High	☐N/A
Account information	☐1-Low	☐2-Medium	☐3-High	☐N/A
Purchase/transaction history	☐1-Low	☐2-Medium	☐3-High	☐N/A
Accept online credit/debit card payments	☐1-Low	☐2-Medium	☐**3-High**	☐N/A
Online enrollment or application forms	☐1-Low	☐2-Medium	☐3-High	☐N/A
Financial information	☐1-Low	☐2-Medium	☐**3-High**	☐N/A
Medical records	☐1-Low	☐2-Medium	☐**3-High**	☐N/A
Legal documents	☐1-Low	☐2-Medium	☐3-High	☐N/A
List other sensitive information located on customer-facing Website(s)				

VI. Network Security

All of the sensitive information assets listed in the previous section must be protected.
This section will help to define your company's network security strengths and vulnerabilities, and assign a risk rating for the level of security provided.
If you use a third-party to manage networks, you may need to verify controls with them.

Basic Network Controls			
Do you use firewalls, routers and other devises to protect your network?	☐Yes	☐No	☐N/A
Are firewalls, routers, and other devices securely configured to control access?	☐Yes	☐No	☐N/A
Have the following configuration steps been completed?			
Changed the default admin passwords	☐Yes	☐No	☐N/A
Removed unneeded services	☐Yes	☐No	☐N/A
Do you use updated anti-virus and anti-spyware software:			

On all desktop computers with automatic update	☐Yes ☐No ☐N/A
On all computers and servers with automatic update	☐Yes ☐No ☐N/A
To Scan all incoming email	☐Yes ☐No ☐N/A
Do you regularly update software and security patches:	
On all desktop computers with automatic update, where available	☐Yes ☐No ☐N/A
On all computers and servers with automatic update, where available	☐Yes ☐No ☐N/A

Secure Access to Information: Network Servers	
How do you limit access to your network? (Check all that apply)	
☐ No controls, or use shared log on	
☐ Unique user ID and password	
☐ Unique user ID, password, plus additional authentication is required	
Do you use employee permission controls to restrict access to authorized users?	☐Yes ☐No ☐N/A
Is employee access to the network monitored?	☐Yes ☐No ☐N/A
Are unsuccessful log on attempts monitored?	☐Yes ☐No ☐N/A
Is email used to send or receive sensitive information?	☐Yes ☐No ☐N/A
If so, is the email encrypted?	☐Yes ☐No ☐N/A

Secure Access to Information: Wireless and Remote Access	
Do you allow remote access to your network?	☐Yes ☐No ☐N/A
If Yes, how do your secure your remote access? (Check all that apply)	
☐ Unique user ID and password ☐ VPN or similar ☐ VPN with additional authentication required	
Do you require minimum security standards (anti-virus, firewall, etc) for computers with remote access?	☐Yes ☐No ☐N/A
Do you have a wireless network?	☐Yes ☐No ☐N/A
If Yes, is the wireless network secured? (Note, WEP is not a secure encryption protocol for wireless networks.)	☐Yes ☐No ☐N/A
Is the wireless network for “guest” access and is it on a separate subnet from the rest of the network?	☐Yes ☐No ☐N/A

Secure Access to Information: Public-Facing Website	
Do you have sensitive customer information on your Website? (If no, skip this section)	☐Yes ☐No ☐N/A
Is your public-facing Website hosted by a third party vendor?	☐Yes ☐No ☐N/A
If yes, are third party vendor contracts up-to-date and cover all expectations for security?	☐Yes ☐No ☐N/A
How is your public-facing Website(s) secured? (Check all that apply)	
☐ Unique user ID and password	
☐ Additional authentication is required	
☐ Firewall	
☐ Encrypted with Secure Socket Layer (SSL)	
☐ Other	

Secure Access to Information: Payment Card Handling	
Do you accept credit cards and other payments from your Website? (If no, skip this section)	☐Yes ☐No ☐N/A
If yes, Is the payment process PCI certified?	☐Yes ☐No ☐N/A
Do you use a third party vendor(s) to process credit cards and other payments from customers?	☐Yes ☐No ☐N/A
If yes, are third party vendor contracts up-to-date and cover all of expectations for security?	☐Yes ☐No ☐N/A
If yes, does your business follow PCI, SSAE 16, SAS70, HIPAA or other guidelines for "controlling employee access" to this information?	☐Yes ☐No ☐N/A

Storage of sensitive information		
Do you store sensitive information on any of the following media? If Yes, is it encrypted?	Sensitive Data	Encrypted
Network files/database	☐Yes ☐No	☐Yes ☐No
Desktop computers	☐Yes ☐No	☐Yes ☐No
Laptops/tablets	☐Yes ☐No	☐Yes ☐No
Mobile phones/devices	☐Yes ☐No	☐Yes ☐No
Flash drives, CD, DVD, or other portable storage	☐Yes ☐No	☐Yes ☐No
Backup tapes and other media	☐Yes ☐No	☐Yes ☐No
Cloud data storage	☐Yes ☐No	☐Yes ☐No
Other:_____	☐Yes ☐No	☐Yes ☐No

Disposal of Information	
Do you remove unnecessary files or data at least annually, especially sensitive information?	☐Yes ☐No ☐N/A
How is sensitive information permanently destroyed? (Check all that apply)	
☐ Electronic files and data are securely removed	
☐ Paper checks and records with sensitive data is cross-shredded	
☐ Third party vendor is used to shred documents or remove data	
☐ Data is permanently removed before equipment is sold or discarded	
Are there regular audit reviews of the company's disposal policies?	☐Yes ☐No ☐N/A

Data Breach Loss/Back up/Disaster Recovery	
Do you have alternative (redundant) hosting facilities in the event of failure?	☐Yes ☐No ☐N/A
Do you have an acceptable procedure for back up of your data?	☐Yes ☐No ☐N/A
Where is your back up data stored? (Check all that apply)	
☐ On a redundant storage device on site	
☐ Backup media is moved to a secure off-site storage location	
☐ Online backup provider	
Is the backup information encrypted? (Check all that apply)	☐Yes ☐No ☐N/A
☐ The backup media is encrypted (tapes, hard drives, etc.)	
☐ Online backups use a secure connection (e.g. SSL)	
☐ Backups are encrypted at rest (e.g. redundant storage device or online backups are encrypted on the server)	

Intrusion Systems	
Is there an intrusion detection or prevention system used in the company's network?	☐Yes ☐No ☐N/A
Is a vulnerability scan or penetration test performed on all Internet-facing systems?	☐Yes ☐No ☐N/A
List other network security issues for your business:	

Rate your Network Security risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:							
Least Secure	☐1	☐2	☐3	☐4	☐5	Most Secure	
Reason for the rating:							

List areas of high risk (threats):	List new controls needed: