

## TRUSTe Security Guidelines 2.0



### Summary

Increasing criminal attacks on consumer and employee data have wrought a high price on individual privacy and trust. In accordance with TRUSTe's broad mission to increase respect for personal identity and information, we are therefore pleased to issue these revised Data Security Guidelines for use as a resource by our licensees and other members of the public. Meaningful protection of consumer privacy depends on a foundation of responsible data security practices.

This new version of the Guidelines provides additional information in three important areas of data security. First, more attention has been given to web application security. Additional guidelines for mobile devices have also been added. Finally, preparation for possible data breaches has been addressed in two new sections.

Security standards are not "one size fits all." Responsible, commercially reasonable standards vary, depending on such factors as a company's size and complexity, industry category, sensitivity of data collected, number of customers served, and use of outside vendors. These Security Guidelines are divided into five categories of safeguards: Parts 1, 2, and 3 address overall administrative, technical, and physical safeguards. Parts 4 and 5 are substantially new sections and address incident response plans and breach notice processes, respectively. All recommended practices are presented in a checklist form so that companies can assess their own risk levels and adopt the practices most appropriate to their particular circumstances.

## Introduction

### Security Enables Privacy Protection

Meaningful protection of consumer privacy depends on a foundation of responsible data security practices. In accordance with TRUSTe's broad mission to increase respect for personal identity and information, we are therefore pleased to issue Data Security Guidelines for use as a resource by our licensees and other members of the public. We hope these Guidelines will help facilitate internal discussion between privacy and security groups, assist companies as they initially draft their internal security policies, and be useful as a checklist to confirm and perhaps doublecheck existing policies. These practices are not intended as mandatory procedures for TRUSTe licensees.

This version of the Guidelines supplements our previously recommended practices in the areas of web application security, mobile device security, and best practices related to data breach incident response, including potential public notification of any such breach.

Web application security focuses on the ways that sites might be vulnerable to hackers. Web applications are used to perform most major tasks or website functions. They include forms that collect personal, classified, and confidential information such as medical history, credit and bank account information and user feedback.

No one on the Internet is immune from security threats. In the race to develop online services, web applications have often been developed and deployed with minimal attention given to security risks, resulting in a surprising number of corporate sites that are vulnerable to hackers. The consequences of a security breach are great: loss of revenues, damage to credibility, legal liability, and loss of customer trust. Web application security is a significant privacy and risk compliance concern and organizations should identify and address web application security vulnerabilities as part of an overall web risk management program.

We have also supplemented recommended safeguards as they relate to mobile devices, particularly those on which sensitive information is stored. While this is not a new area of concern, mobile devices have surfaced as a point of vulnerability for many businesses, as evidenced by a number of publicly-acknowledged breaches traceable to, for example, stolen laptops containing sensitive information. As technology develops, new methods of transmitting, receiving and storing personal data via mobile devices are created. This poses new problems for privacy protection. The Guidelines set forth some simple steps that can assist companies in determining how to handle data security on mobile devices.

Finally, two sections relating to incident response in general, and specifically breach notices, have been added. Because of the many data breaches recently, many states have now enacted legislation requiring companies to protect data and notify affected individuals. As companies contemplate these legal requirements, as well as a desire to maintain customer trust even in the face of data breaches, these Guidelines set forth some recommended steps to help companies be prepared in the event of a data breach.

### Using the Guidelines

Security standards are not "one size fits all." Responsible, commercially reasonable standards vary, depending on such factors as a company's size and complexity, industry category, sensitivity of data collected, number of customers served, and use of outside vendors.

The Security Guidelines are drafted in checklist form so that companies can assess their own risk levels and adopt the corresponding appropriate level of recommended safeguard practices. Larger, more complex companies which handle data with the highest level of sensitivity will likely find it appropriate to adopt all the recommended practices, while a smaller company, collecting less sensitive information, may conclude

that adopting only a subset of these controls will still enable it to have a security program appropriate to the nature of the data it collects and handles.

These Security Guidelines are divided into five categories of safeguards: Parts 1, 2, and 3 address overall administrative, technical, and physical safeguards. Parts 4 and 5 address incident response plans and breach notice processes, respectively. Administrative controls include, for example, drafting a written internal security policy, training employees, conducting ongoing security risk assessments, and establishing procedures in connection with external third parties (including vendors) with whom data is shared. Technical measures include controlling employee access to sensitive information on a need-to-know basis, establishing good password practices, ongoing monitoring to assess threats and vulnerabilities, ensuring web application security, and establishing incident response procedures. Physical controls include practices such as monitoring legitimate access to data, establishing physical access controls, and securing one's data facilities. Finally, incident planning and response controls include creating a response team, creating a response plan, and formulating a breach notification policy.

Following each of these three main categories, the user will find different types of safeguards, each followed by a number of more detailed supporting directives.

For the user's convenience, the Guidelines are presented in checklist form, with each recommended control accompanied by checkboxes which the user can fill in with his or her own assessment of whether the practice is appropriate and relevant to the user's particular company, as follows:

✓Should be required – A check in this category means that you believe the practice or procedure should be implemented within your organization to achieve reasonable data protection levels.

✓Should be optional – A check in this category means that you believe the practice or procedure will be useful, but may not be appropriate within your organization to achieve reasonable data protection levels.

✓Not relevant – A check in this category means that you believe the practice or procedure will not be useful within your organization for purposes of data protection.

## Guiding Principles

We recognize that companies may achieve reasonable security through other measures, not included within the Guidelines. While the Guidelines rely upon other learned information security standards such as ISO 17799 and the Payment Card Industry (PCI) Guidelines, and are informed by regulatory requirements such as those imposed by the Gramm Leach Bliley Act and HIPAA, they are not intended as a comprehensive list of all leading security measures. Rather, the Guidelines are intended to provide a relatively non-technical, high level overview of responsible security practices. For those users wishing a more detailed or technological focus, the Guidelines also contain links to an array of information security websites which some users will find helpful.

We anticipate that the Guidelines will evolve over time to reflect emerging technologies and business issues that may impact the safety, security and quality of sensitive or confidential information used by TRUSTe's licensees. Finally, we welcome suggestions and comments via email to [policylegal@truste.org](mailto:policylegal@truste.org).

## Sources

Following are the main sources used to draft the attached Guidelines:

International Organization for Standardization (ISO) 17799. ISO-17799 is an International recognized Information Security Management Standard first published in December 2000, derived from British Standard 7799 Parts I and II.

Visa USA Cardholder Information Security Program (CISP). Established in June 2001, the program is intended to protect Visa cardholder data to ensure that members, merchants, and service providers maintain reasonably high information security standard. In addition to the CISP “digital dozen,” we included new features from the PCI Data Security Guidelines.

Organisation for Economic Co-Operation and Development (OECD), Guidelines for the Security of Information Systems. In addition, we reviewed various papers published by the Business and Industry Advisory Committee (BIAC) to the OECD.

## Acknowledgments

TRUSTe would like to acknowledge the many experts we consulted in revising these Guidelines.

Dr. Larry Ponemon of the Ponemon Institute was instrumental in developing these Guidelines. Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government.

[www.ponemon.org](http://www.ponemon.org)

Watchfire provided input and guidance in developing the Web application security guidelines.

Watchfire is a provider of Online Risk Management software and services to monitor and report online security, privacy, quality, accessibility, and compliance risks. For more information on Watchfire and its web application security expertise please visit:

<http://www.watchfire.com/securityzone/default.aspx>

Joanne McNabb, Chief, California Office of Privacy Protection, provided guidance in connection with the new incident response sections. The California Office of Privacy Protection assists individuals with identity theft and other privacy-related concerns; provides consumer education and information on privacy issues; coordinates with local, state and federal law enforcement on identity theft investigations; and recommends policies and practices that protect individual privacy rights.

[www.privacy.ca.gov](http://www.privacy.ca.gov)

TRUSTe would also like to recognize the contributions of Ernst & Young and ChoicePoint Inc.

## Part 1: Administrative Controls

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
1.0	Establish a security committee.			
1.1	Ensure that the committee is composed of cross-functional members representing different parts of the organization.			
1.2	Create a charter for the security committee.			
1.3	Designate an executive sponsor for security function. The sponsor should also serve as a member of the cross-functional committee.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
2.0	Establish a formal, written security policy and detailed standard operating procedures.			
2.1	Ensure that the policy applies to the entire organization or that appropriate policies exist to cover the various operations in the organization, and that they are integrated with other enterprise policies. Ensure that appropriate policies also apply to your internal and external websites.			
2.2	Align the policies with other compliance policies, especially those for privacy and secure vendor relationships. Before creating your policies, determine regulatory compliance needs as relevant to the data and customers.			
2.3	Ensure that versions of the security policy are coordinated and rigorous version control is exercised.			
2.4	Periodically review the security policy and standard operating procedures, revising them as necessary based on changing business, technology and environmental conditions.			
2.5	Disseminate the security policy and detailed standard operating procedures to all relevant stakeholders within the organization. Consider developing an externalizable version of the policy and for outside stakeholders of the organization, including outside contractors agents.			
2.6	Provide appropriate information on how you secure information to users on your websites through a link on each page. Consider including this summary in your privacy statement.			

## Part 1: Administrative Controls, cont.

3.0 Conduct ongoing security risk assessments.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
3.1	Identify and prioritize security risk threats and vulnerabilities. Consider, at a minimum, risks in these areas: employee training and management; information systems; and prevention, detection and response to attacks or other systems failures.			
3.2	Prioritize resource allocation and spending based on prioritized risk areas.			
3.3	Periodically review risk assessments and revise them as necessary, especially in response to business, technology and environmental changes.			

4.0 Require a system security plan for every major system and network.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
4.1	Conduct a periodic review of system security plans and revise them as necessary.			
4.2	Ensure that plans and policies for security include periodic review and control over endpoints such as desktop PC's, laptops, PDA's, and other devices which connect to sensitive networks or systems (including Bluetooth technology).			
4.3	Require system interconnection agreements.			
4.4	Require user system access agreements.			
4.5	Conduct periodic review of system interconnection agreements and revise them as necessary.			

5.0 Establish contingency plans, including maintenance of access controls.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
5.1	Establish business continuity plan.			
5.2	Establish disaster recovery plan.			
5.3	Establish personnel emergency plan.			
5.4	Conduct periodic review and test of contingency plans and revise them as necessary.			

6.0 Integrate security throughout the system life cycle, including:		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
6.1	Requirements definitions.			
6.2	Design/procurement procedures.			
6.3	Testing and maintenance procedures.			

## Part 1: Administrative Controls, cont.

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
7.0	Establish formal data backup processes.			
7.1	Ensure that data backup includes the maintenance of current access controls.			
7.2	Conduct periodic review and test of data backup processes and revise them as necessary.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
8.0	Establish security auditing process.			
8.1	Conduct periodic reviews of all security controls through internal or external audit. Include web applications, as well as host, network and user accounts as part of the audit.			
8.2	Conduct mock reviews to test the organization's ability to respond to threats (including vulnerability to social engineering).			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
9.0	Document all system and network configurations.			
9.1	Establish a formal configuration/change control process (including vulnerability identification and patching), with pre-production testing.			
9.2	Document and classify all sensitive information (data inventory).			
9.3	Document formal and appropriate rules of behavior, acceptable use and confidentiality agreements for all personnel with access to sensitive information.			
9.4	Document all appropriate separation of duties (e.g., system administrators and security administrators should not be the same person).			
9.5	Document routine and emergency access termination procedures.			
9.6	Document a formal incident response capability.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
10.0	Establish employee awareness and training program.			
10.1	Establish a certification and accreditation (C&A) process for employees with access to major systems.			
10.2	Require all employees to undergo basic initial and refresher security training. Track and document completion of training.			
10.3	Support continuing professional training and education for security specialists.			

**Part 1: Administrative Controls, cont.**

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
11.0	Establish special procedures for outsourced IT or data management activities.			
11.1	Perform vendor due diligence before sharing sensitive or confidential information, including all personally identifiable consumer or employee data.			
11.2	Perform a site audit of the vendor's data center to determine adequacy of security infrastructure.			
11.3	Obtain certification from the vendor that they are in compliance with the customer's privacy and data protection obligations as required by law or stated policies.			
11.4	Impose contractual control over vendors' data use and practices.			
11.5	Perform periodic or random audits of the outsourcing vendor.			
11.6	Whenever feasible, determine the adequacy and competence of the outsourced vendor's key personnel (especially those individuals who are responsible for handling or managing sensitive personal information).			

## Part 2: Technical Security

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
1.0	Control access to information that resides on data storage devices such as servers, desktop PCs, laptops, and PDAs.			
1.1	Use unique ID or username for all system users. Ensure that neither Social Security nor account numbers are used as an ID or username.			
1.2	Use authentication mechanisms, such as passwords, tokens, and/or biometrics.			
1.3	Require system administrators to use regular user accounts for work that does not need enterprise-wide system or security administration privileges.			
1.4	Assign access privileges based on a need to know (the level of access should only relate to job function and be not based on organizational position or rank).			
1.5	Whenever feasible, utilize a two-factor authentication procedure before granting access to a user's sensitive information.			
1.6	When possible, implement a method for online service requests concerning changes in usernames and passwords.			
1.7	Force appropriate session timeouts, such as 15 minutes or less, if idle.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
2.0	Establish password usage policy that encompasses the following rules:			
2.1	Whenever feasible, use a minimum of six digit alpha-numeric format. Instruct users to create such passwords during a periodic password change process.			
2.2	Prohibit passwords based on account number, username, real name, Social Security number, or publicly available personal details (birthdays, names of children or pets, etc.).			
2.3	Restrict password reuse.			
2.4	Establish a formal user authentication process for resetting passwords. When possible, make password change or reset option available from the login page. Allow users to update their password hints or questions.			
2.5	When sending a registration confirmation or other type of welcome email, provide only the username within the email and implement a password reset feature on the web site.			
2.6	Username and passwords should not be sent together within the same email.			
2.7	Force password expiration.			
2.8	Establish lost/stolen laptop procedures, including password cancellation.			

## Part 2: Technical Security, cont.

3.0	Control access to information that can be displayed, printed, and/or downloaded to external storage devices, especially desktop PCs, laptops or PDAs.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
3.1	Have operating controls that restrict downloads of sensitive information without proper identification. (See Appendix for sensitive data classifications.)			
3.2	Have screen savers and screen shields to minimize the display of sensitive data to unauthorized users.			
3.3	Have shutdown controls when computers are idle or inactive.			
3.4	Whenever feasible, only allow read-only access rights when using remote computers or wireless devices to enter the organization's network or enterprise system.			
3.5	As much as possible, limit the use of personally identifiable information on laptops. Where such use is essential, ensure that data is encrypted or, at a minimum, that such laptops are protected by something stronger than a password.			
3.6	Set up periodic disk clean-up reminders to help eliminate temporary backups and empty recycle/trash bin. Consider reflecting this practice in your company document retention/deletion plans.			

4.0	Monitor user accounts to identify and eliminate inactive users, specifically:	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
4.1	Accounts that have been inactive for 60 days should be automatically terminated.			
4.2	Accounts of terminated employees and contractors should be shut down within 24 hours.			
4.3	Regularly cross-check user accounts against HR records to ensure that access by former employees has been terminated.			

5.0	Ensure sufficient safeguards over the transmission and storage of data, including:	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
5.1	Use reasonable encryption methods when transmitting or receiving sensitive information, especially when sent or received over the public Internet. Ensure that you employ at least 128-bit encryption.			
5.2	Use wireless encryption protocol (WEP) when transmitting or receiving sensitive information from PDAs, Web phones, laptops, and emerging devices that use Bluetooth connection technologies.			
5.3	Use reasonable encryption methods for storage, especially when maintaining sensitive information on servers, desktop PCs, and laptops.			
5.4	Use VPN software to authorize and encrypt traffic from authorized devices, and ensure that VPN access has adequate controls and is monitored.			
5.5	Use configuration monitoring tools to flag storage devices that are removed from the network or enterprise system.			
5.6	Restrict the downloading of sensitive personal information from central storage devices onto personal computers or wireless storage devices.			

## Part 2: Technical Security, cont.

6.0 Configure all servers, desktop PCs, and laptops prior to use, including:		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
6.1	Disable unused ports.			
6.2	Install/enable automatic screen locks to prevent access after a certain period of inactivity.			
6.3	Change all vendor-supplied default passwords.			
6.4	Ensure that wireless encryption protocol (WEP) is enabled prior to allowing wireless devices to be connected to enterprise systems or networks.			
6.5	Treat all internal wireless connections as external connections.			
6.6	Routinely check for unauthorized external access capability, including wireless access points.			
6.7	Confirm that default software installations and configurations are appropriate for your security needs, including as appropriate changing default passwords and appropriately adjusting security parameters.			

7.0 Firewalls should be configured to provide maximum protection over information, balancing business needs with reasonable security.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
7.1	Establish a formal process for approving and testing all external network connections.			
7.2	Establish a firewall at each Internet connection.			
7.3	Establish a firewall between any DMZ and Intranet connection.			
7.4	Utilize multi-layered firewall configurations to protect sensitive information. (See Appendix for sensitive data classification).			
7.5	Validate firewall configurations with vulnerability tools available from vendors.			
7.6	Conduct application level assessments to ensure application and database security.			

8.0 Install and configure anti-spyware software to provide maximum protection of sensitive information on all servers, desktop PCs, and laptops.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
8.1	Ensure automatic downloads and updates to enterprise system or network.			
8.2	Ensure automatic downloads and updates to desktop PCs, laptops and PDAs that are connected to the enterprise system or network.			
8.3	Perform frequent scans of data storage using enabling technologies to detect, quarantine, and remove viruses, worms, and Trojans.			
8.4	Instruct employees not to download unknown attachments that could contain viruses, worms, spyware or keystroke loggers potentially giving unauthorized individuals access to the company's network. This applies to the user of any computer that has access to the organizational network, including the home computer of a telecommuting employee or a traveling employee logging in from a hotel or other public access point.			

## Part 2: Technical Security, cont.

9.0 Implement security software updates and patches in a timely manner.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
9.1	Install security patches within one month of release date.			
9.2	Establish a process to identify newly discovered security vulnerabilities by subscribing to alert services that report current external threats.			
9.3	Ensure that all servers are up-to-date with respect to application version and security patches. Additionally, scan servers for configuration issues.			

10.0 Enhance the security of your websites.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
10.1	Prevent your web pages from being delivered into frames by another site.			
10.2	Ensure that all web pages that enable users to transmit or receive sensitive information use https:// or another security method such as SSL, Web seal, or certificates.			
10.3	Mask account and credit card numbers.			
10.4	Clearly label links to third-party sites to ensure users know they are leaving your site by following the link.			
10.5	Make a secure email form available to prospective users.			

11.0 When developing software, create and implement security-focused web application development procedures.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
11.1	When possible, use desktop tools to validate and correct code issues.			
11.2	Implement quality assurance and testing procedures. This would include detecting, measuring, and managing security defects as part of QA.			
11.3	Include training on security tools as part of the software development life cycle.			
11.4	Develop procurement and acceptance procedures to apply when purchasing third party software. Validate vendor and third party code for acceptable risks.			
11.5	Develop staging and integration procedures. Make sure project owners evaluate application risks before public release.			
11.6	Conduct ongoing application assessments for existing production code and one for each maintenance cycle release.			

## Part 3: Physical Controls

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
1.0	Monitor legitimate use and access.			
1.1	Conduct surveillance of unusual Internet activities (such as Web browsing or use of peer-to-peer file sharing software). Be sure to consider any applicable legal restrictions on doing so, however.			
1.2	Conduct surveillance of unusual email.			
1.3	Perform periodic or random reviews of documents and software contained on company issued laptops computers and PDAs.			
1.4	Monitor software licenses for inactive or pirated copies.			
2.0	Establish physical access controls.			
2.1	Install PIN devices, smart cards, and/or biometric readers at physical entrances to the data center.			
2.2	Restrict physical access to the data center to only those people who have a legitimate business need.			
2.3	Establish a method to recognize employee access rights and privileges.			
2.4	Keys and passes, especially master keys, should be carefully controlled with frequent reviews and reconciliation.			
2.5	Establish a method to terminate access rights once employee or contractor illegal activities are detected or strongly suspected.			
2.6	Establish a method to differentiate employees from contractors.			
3.0	Install secure checkpoint review and monitoring procedures.			
3.1	Implement a data center security or reception desk, especially at the entrance where sensitive or confidential information is housed or is accessible.			
3.2	Implement a formal process for granting access to those areas and for maintaining the list of people with physical access.			
3.3	Identify and monitor the movement of all visitors by using temporary badges or machine readable devices (such as RFID tags).			
3.4	Take appropriate security precautions in areas where access to sensitive data may be had. These can include special locks, security personnel, access controls, and other features. In the most sensitive areas, such as data centers, consider installing motion detectors, micro-switches and pressure pads or other equipment or measures in data centers to indicate when doors are opened or rooms entered.			
3.5	Install closed circuit television to monitor all entry points.			

### Part 3: Physical Controls, cont.

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
4.0	Secure the data facility, including all storage devices and computer equipment.			
4.1	Locate loading docks or delivery areas in a remote area of the building far away from areas processing or storing confidential information.			
4.2	Control or limit access to junction boxes and telecommunication lines that enter or exit the data center.			
4.3	Rooms that house especially sensitive equipment should have no external walls, doors, windows or sky lights.			
4.4	The area designated for the enterprise system or networks should be designed and built to support the organization's requirement for information security.			
4.5	Secure cages and racks should be used to protect sensitive equipment. These should be locked routinely and keys carefully controlled.			
4.6	Use locked cabinets to store printouts containing sensitive or confidential information.			
4.7	Require documented approval by the data center's management before disconnecting or removing storage devices from the central IT configuration or system network.			
4.8	Maintain logging procedures for all removable storage devices and media, including magnetic tapes.			
4.9	Keep unused laptops and other mobile devices in a locked location to prevent theft.			
4.10	Consider technologies and implementations that can effectively terminate remote access in case of compromised mobile equipment.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
5.0	Install and maintain reasonable environmental protections over all data center assets.			
5.1	Install raised floor to protect equipment in the data center.			
5.2	Install and maintain fire detection and suppression systems.			
5.3	Implement uninterruptible power supply (UPS).			
5.4	Use surge protectors on all equipment.			

## Part 4: Incident Response Plan

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
1.0	Establish an internal incident response team.			
1.1	Create an internal response team with the expertise, authority, and resources to act quickly in case of a security incident. Possible responsibilities will include investigation of the cause and parameters of the incident; containing and controlling of the incident; data recovery; decisions about external communications to law enforcement, impacted individuals such as customers or employees, and/or the media; and subsequent debriefing after any incident. Assuming this is a different group than is drafting your incident response policies, the two groups must have a clear working relationship and at least some overlap.			
1.2	Consider including representatives from these departments: IT, security, privacy, legal, marketing/sales/customer relations (in case customer data is involved), human resources (in case employee data is involved), and media relations. The team may also include outside experts under retainer or contract.			
1.3	Establish clear roles and responsibilities for all team members.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
2.0	Establish a formal, written breach response plan.			
2.1	Inventory any existing response or investigative policies or related procedures.			
2.2	Implement an internal escalation, notification, and decision making process to be followed in case of a potential security breach. If an established process already exists, review for completeness and currency.			
2.3	Implement a forensic analysis capability to support incident investigations, ensuring that potential evidence is not compromised. Small or medium companies with less internal technical expertise may wish to retain a third party expert for this function.			
2.4	Consider consulting with law enforcement resources in advance of any incident to understand relevant procedures and what resources they may bring to bear, should a breach occur. Appropriate law enforcement resources may include your local high tech crimes task force, FBI, Secret Service, US Postal Service, and the National Infrastructure Protection Service.			
2.5	Establish a process for assessing whether to contact law enforcement in case of a breach, and for making such contact.			

## Part 4: Incident Response Plan, cont.

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
3.0	Develop a process for reporting and escalating incidents.			
3.1	Emphasize that all suspicious activity and potential breaches should be reported internally, and ensure that all employees understand the internal notification process, specifically, who within the company they are to report a potential incident to. “Incidents” include unauthorized access, acquisition or use. Emphasize that both internal and external unauthorized access should be reported.			
3.2	Develop internal systems and processes to identify breaches and potential breaches, assessing what information may have been accessed or acquired and by whom. Systems and processes may also raise alerts when inadvertent access to information is made by unauthorized employees.			
3.3	Implement a specific notification and escalation process for when a laptop or other mobile device is lost, missing or stolen. Establish a procedure to understand what information was on the laptop, how it was secured and what access rights may exist; modify end-user access rights as needed.			
3.4	In your role as a principal and the party with the customer or employer-employee relationship (the “data owner”), you should require, e.g., via contract, that any outside vendors (“data custodians”) notify you immediately upon detection of a breach involving data that you have provided to them or otherwise made accessible to them. Require such vendors to keep you informed of the investigation process and progress and to work cooperatively with you in any investigation or other follow-up activity.			
3.5	Conversely, if you are a vendor, be aware of any contractual or legal obligation you may have to notify your principal of a breach involving data they have provided to you. Consider providing such notice once you have established the facts of the breach, regardless of whether you have a technical obligation to do so.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
4.0	Establish a periodic and post-incident review and re-testing process.			
4.1	Establish a post-incident internal debriefing process, including what went wrong, lessons learned and next steps.			
4.2	All incident plans, policies, processes, and related systems should be appropriately documented and understood by the responsible employees. Communicate these through training and updates as appropriate.			
4.3	All incident plans, policies, processes, and related systems should be reviewed, tested and updated, both periodically and after any incident.			

## Part 5: Breach Notice Processes

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
1.0	Establish a process for assessing whether a breach notice is either legally mandated or otherwise appropriate.			
1.1	Consider establishing a breach notice subgroup of your incident response team—or designate an individual—tasked with assessing, in case of a breach, whether the need for a breach notice has been triggered and, if so, carrying out the breach notice process. If assigned to an individual, designate a substitute in case of vacation, illness or absence for any reason.			
1.2	Familiarize yourself with applicable state breach notice and other privacy-related laws, as well as any relevant international laws. Such laws mandate, under certain circumstances, that you notify individuals whose personally identifiable information has been accessed or acquired in an unauthorized fashion. Factors impacting such legal requirements will include the nature of a breach, the type of information involved, and the jurisdictions impacted. (Note that federal legislation is also pending.)			
1.3	Establish a process for determining whether notice is legally mandated or otherwise appropriate.			
1.4	If notice is not legally mandated, consider nonetheless providing notice, particularly where there has been unauthorized access or acquisition of data that could reasonably result in material harm to the subject of the information.			
1.5	When evaluating such a possibility of material harm, consider using the “sensitive data” category as defined in the “Data Categories” chart at the bottom of these Guidelines.			
1.6	Consider establishing, also, what less-sensitive categories of data will likely not trigger a breach notice. Depending on applicable legal requirements, examples might include email addresses not linked to any other personally identifiable information.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
2.0	Establish a process for determining who to notify, once the need for a breach notice has been triggered.			
2.1	Determine who has been affected, and notify each affected individual when possible. Doublecheck the list of recipients before sending.			
2.2	Try to ensure that only those individuals whose personally identifiable information was compromised are included in the group to be notified. If you cannot determine the exact individuals affected, consider notifying all members of the group affected if the likelihood of material harm outweighs the uncertainty that the individuals were affected.			

		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
3.0	Establish a process for communicating a breach notice.			
3.1	Consider potential communication channels for different circumstances, e.g., your plan may be different for an employee vs. a customer data breach.			
3.2	Consider available options, should you not have complete contact information for all impacted individuals.			

## Part 5: Breach Notice Processes, cont.

4.0 Considerations that affect the timing of a breach notice include:		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
4.1	In general, notify affected individuals as soon as reasonably possible after a breach is discovered, unless law enforcement officials indicate that notice would impede their investigation. Note that the California Office of Privacy Protection recommends notification within ten days once a breach has been confirmed.			
4.2	If you have reported the breach to law enforcement, ask them to inform you when it is safe to notify affected individuals. Send out notice as soon as practicable and in compliance with existing notification laws when so informed. Consider appointing a member of the response team to follow up with law enforcement in order to find out when it is safe to notify the affected individuals. When possible, get such confirmation in writing.			
4.3	Send the notification in an appropriate manner to the intended audience. In consumer notification cases, consider notice by traditional mail and by email where appropriate.			
4.4	Consider the option of giving general public notice, on your website and/or through major media, where the group to be notified is very large or it is otherwise appropriate.			

5.0 Educate and coordinate with your own and other potential resources.		SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
5.1	Educate your call center staff or other customer service employees about the breach so they can provide knowledgeable assistance. Consider having assistance available evenings and weekends.			
5.2	If the breach involves financial information, consider notifying credit reporting agencies before sending out notice of a breach to a large number of individuals, so they can prepare for the consequent inquiries. (You will find information about the major CRAs at <a href="http://www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html">http://www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html</a> .) However, do not delay notice to individuals because of cooperation with credit reporting agencies.			

## Part 5: Breach Notice Processes, cont.

6.0	Content of breach notice communication.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
6.1	Consider carefully the content of any breach notice communications, and focus on providing the most useful information possible.			
6.2	In the case of consumer breach, notification should include: (a) the date of the breach; (b) what information was accessed and pertinent details about the breach; (c) remedial actions taken; (d) your toll-free number for individuals to call to learn more, including whether or not that individual's data may be at risk; (e) how affected individuals may protect themselves against the possibility of identity theft; and (f) contact information for major credit reporting agencies.			
6.3	Consider providing further information that might be helpful for those who believe they maybe a victim of identity theft. For example, including a brochure about how to set up credit monitoring or how to read a credit report could be helpful.			
6.4	Consider offering free credit monitoring services for one year to affected individuals, particularly if the incident involved Social Security or Driver's License numbers. (When considering making such an offer, note that often only about 25% of consumers will accept such an offer.)			
6.5	Consider providing links on your website to resources such as the following: the three major credit reporting agencies (available via an FTC "FAQ" at <a href="http://www.ftc.gov/bcp/online/edcams/gettingcredit/faqs.html">http://www.ftc.gov/bcp/online/edcams/gettingcredit/faqs.html</a> ); to government agency resources such as this FTC identity theft consumer alert ( <a href="http://www.ftc.gov/bcp/online/pubs/alerts/info-compartr.htm">http://www.ftc.gov/bcp/online/pubs/alerts/info-compartr.htm</a> ); and/or to identity theft resources such as the Identity Theft Resource Center ( <a href="http://www.idtheftcenter.org/">www.idtheftcenter.org/</a> ) or the Privacy Rights Clearinghouse ( <a href="http://www.privacyrights.org/">http://www.privacyrights.org/</a> ).			
6.6	You will also find sample breach notices letters provided by the California Office of Privacy Protection available at: <a href="http://www.privacy.ca.gov/recommendations/secbreach.pdf">http://www.privacy.ca.gov/recommendations/secbreach.pdf</a> .			

## Data Categories

When establishing security controls, it is useful to categorize data by level of sensitivity. These are some possible data categories:

### Sensitive Personal Data

Data that is (1) identifiable to an individual person and (2) has the potential to be used to harm or embarrass the data subject.

- Social Security Numbers
- National ID Numbers
- Driver's license number
- Credit Card numbers
- Account numbers
- Passwords, including PINs\*
- Criminal arrests or convictions
- Judgments in civil cases
- Medical information
- Administrative sanctions
- Race, ethnicity, national origin
- Data concerning sexual orientation or activity
- Financial data (such as credit rating)
- Salary & compensation
- Disability status

### Ordinary Personal Data

Data that is identifiable to an individual person but that is generally considered to have a lower level of sensitivity than "Sensitive Data".

- Name
- Telephone # (work & home)
- Address (work & home)
- Email address (work and home)
- Gender
- Marital status
- Number of children
- Date of birth or age
- Citizenship
- Education
- Income range
- Non-medical benefits information
- Purchase history
- Buying patterns
- Hobbies and interests

## Information Security Sites

### Introductory

[http://www.iccwbo.org/home/e\\_business/securing\\_your\\_business.pdf](http://www.iccwbo.org/home/e_business/securing_your_business.pdf)  
[http://www.biac.org/statements/iccp/Final\\_Information\\_Security\\_for\\_Executives071003.pdf](http://www.biac.org/statements/iccp/Final_Information_Security_for_Executives071003.pdf)  
<http://www.ftc.gov/infosecurity/>  
<http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase>  
<http://www.sans.org/top20/>

### General

<http://www.infosyssec.net/>  
<http://www.cerias.purdue.edu/>

### Technical / Alerts / Advisories

<http://www.cert.org/>  
<http://www.cisecurity.org/>  
<http://www.ciac.org/ciac/index.html>

### Magazines / Publications

<http://www.csoonline.com/>  
<http://informationsecurity.techtarget.com/>  
<http://www.scmagazine.com/home/index.cfm>  
<http://www.gsnmagazine.com/>

### AntiVirus / Malware– current alerts

<http://www.trendmicro.com/vinfo/>  
<http://www3.ca.com/securityadvisor/virusinfo/default.aspx>  
[http://www.symantec.com/avcenter/vinfodb.html#threat\\_list](http://www.symantec.com/avcenter/vinfodb.html#threat_list)

### Certification

<http://www.icsalabs.com/index.shtml>

### ID Theft

<http://www.consumer.gov/idtheft/>

### Crime / Government

<http://www.htcia.org/>  
<http://www.infragard.net/>

### Standards

<http://www.nist.gov/>  
<http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>

## Incident Response/Breach Notice Sites

<http://www.privacy.ca.gov/recommendations/secbreach.pdf>  
[http://www.cert.org/csirts/csirt\\_faq.html](http://www.cert.org/csirts/csirt_faq.html)  
<http://www.ncsl.org/programs/lis/CIP/priv/breach.htm>