

DATA PRIVACY + SECURITY CHECKLIST

ChoicePoint

CHOICEPOINT STRIVES TO BE A LEADER IN THE RESPONSIBLE USE OF INFORMATION BY EMPLOYING A COMPREHENSIVE RISK MANAGEMENT PROGRAM FOR PRIVACY, INFORMATION AND PHYSICAL SECURITY, AS WELL AS CUSTOMER CREDENTIALING.

THE FOLLOWING IS A CHECKLIST THAT MAY BE USED AS A GUIDE TO HELP ORGANIZATIONS BUILD THEIR OWN PRIVACY AND INFORMATION SECURITY FRAMEWORKS AND TO ASSIST IN THE EVALUATION OF OTHERS WITH WHOM THEY MAY SEEK TO DO BUSINESS.



ChoicePoint firmly believes that by placing a strong and competitive focus on privacy and information security, and by totally integrating both into our business model, we are a better company and a better business partner.

Since 2005, ChoicePoint has implemented or revised more than 90 policies and procedures related to privacy and information security. We have trained and regularly retrain our entire workforce on these policies and procedures, and we successfully completed 116 independent audits since 2005. We have dedicated significant resources, technology and dollars to further strengthen our privacy and information security framework so you can be confident in our ability to serve your business needs while protecting sensitive information.

Many customers have come to us and asked for guidance with regard to their privacy and information security practices. To support them, we have compiled the attached best practices Data Privacy and Security Checklist. This checklist can be used by your management teams to help develop a privacy and security framework and to evaluate others with whom you may seek to do business.

If you have questions about any part of this document, please contact Alan Rosenberg, vice president of compliance, at 770-752-8933, in our Office of Privacy, Ethics and Compliance, or Aurobindo Sundaram, vice president of information security, at 770-752-3663, in our information security department. Both Alan and Aurobindo and members of their teams would be pleased to participate in discussions that relate to their areas of expertise.

A handwritten signature in black ink, appearing to read "Derek V. Smith". The signature is fluid and cursive, with a large initial "D" and a long, sweeping underline.

Derek V. Smith

Chairman and CEO



Privacy and Information Security Framework

Businesses, nonprofits and all organizations seeking to attain best practices for their privacy and information security programs rely on established internationally recognized frameworks, because of their completeness, consistency and standards-based approach. Due to the scope of privacy and information security, organizations may need to use multiple standards in their custom frameworks. This may include security standards (such as ISO 27002), disaster recovery guidelines (such as those from the FFIEC), privacy standards (such as those from the AICPA) and potentially organization/situation-specific proprietary guidelines (for instance, to appropriately credential/screen customers). Organizations that use deliberate, structured, but flexible processes to create their holistic privacy and information security frameworks will reap the benefits of enhanced risk mitigation.

- Does your organization have a privacy and information security framework that includes administrative, physical and technical safeguards?
- Is it standards based?
- Is one of the standards based upon ISO 27002 (formerly 17799:2005)?
 - ISO 27002 is the internationally accepted standard of good practice for information security.
- Is one of the standards based upon disaster recovery and business continuity such as the Federal Financial Institutions Examination Council (FFIEC)?
 - The FFIEC is a federal interagency body charged with prescribing uniform principles, standards and report forms for the federal examination of financial institutions.
- Is one of the standards based upon privacy such as the American Institute of Certified Public Accountants (AICPA) or Chartered Accountants of Canada (CICA)?
 - The AICPA is a self-regulatory organization of certified public accountants that develops generally accepted accounting principles; the CICA conducts research and supports the setting of accounting, auditing and assurance standards for business, not-for-profit organizations and government.
- Is one of the standards the U.S. Sentencing Guidelines?
- Does your organization base your framework on any separate, proprietary criteria such as customer, employee or vendor credentialing?





Inventory and Access to PII¹ and SPII²

Businesses, nonprofits and all organizations should ensure that they know where consumer Personally Identifiable Information (PII) is stored and processed on their information systems. A periodically updated inventory of PII and Sensitive Personally Identifiable Information (SPII) helps the organizations apply the appropriate controls and protections necessary to prevent unauthorized access to this information. In addition, all organizations should have documented procedures, tools and associated training to control access to PII and SPII, and assist authorized employees in protecting PII and SPII during receipt from customers and consumers, transmission (e.g., via e-mail) and storage.

- Does your organization have written policies/procedures that address collection, use and dissemination of PII and SPII?
- Does your organization have a policy for restricting access to personal information to only those employees, subcontractors and/or agents who need it as part of their job responsibilities?
- Does your organization take inventory on where PII and SPII is stored?
- Is your inventory updated on a regular basis?
- Does your organization limit access to SPII?
- Does your organization truncate and/or mask SPII wherever possible? Incoming and outgoing?
- Does your organization have controls in place to limit SPII transmission via e-mail?



¹ Personally Identifiable Information: Individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name or first initial and last name; (b) a home or other physical address, which includes at least street name and name of city or town; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number with expiration date; (g) date of birth; (h) a driver's license number; or (i) any other information from or about an individual consumer that is combined with (a) through (h) above.

² Sensitive Personally Identifiable Information: Information owned or licensed by the organization that consists of an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or data elements are not encrypted: (1) driver's license or state identification number; (2) Social Security number; or (3) account numbers (such as bank, credit or debit card numbers) when combined with any required security code, access code or password that would permit access to an individual's financial account.



Credentialing (Background Screening)

Credentialing is an essential component of a successful and effective privacy and information security program. As a practical matter, credentialing should focus on three specific constituencies within any organization: (1) employees, (2) customers and (3) vendors/third parties. Through the credentialing of these three groups, an organization is able to mitigate the risk of fraud by verifying employee background information, customer and vendor business credentials, and ensuring permissible regulatory purpose and legitimate business purpose for accessing information products, systems and data. An effective credentialing program for an organization's customers should standardize its credentialing process to ensure consistency and security of the process.

Employees

- Does your organization credential its employees?
- Does the credentialing process require criminal, drug and credit checks?
- Does your organization have a re-credentialing program for employees that includes a criminal background check at least every three years?

Customers

- Does your organization credential its customers?
- Does your organization centralize its credentialing of customers to ensure consistency and security of the process?
- Does your organization follow a credentialing checklist or process that verifies each customer's legitimacy and permissible purpose? Is there a scoring process?
- Does your organization require and conduct site inspections of its customers? Is there a scoring process?
- Does your organization require that each customer pass its credentialing process?
- Does your organization require that each customer pass its site visit process?
- Does the credentialing process/checklist undergo a separate quality control review for each customer?
- Does your organization re-credential its customers?

Vendors

- Does your organization assess/credential its vendors?
- Does your organization re-credential its vendors? How frequently?
- Does the credentialing process for vendors who will have access to sensitive information require background checks?



Corporate Accountability

Accountability refers to the obligations that organizations have to shareholders, customers, employees, consumers and other stakeholders. In the privacy and information security context, accountability is critical to the success of a robust privacy and information security framework. In order to establish an enterprise-wide culture of accountability, there must be a firm commitment from the leadership of the organization coupled with an insistence on transparency that reveals to stakeholders an organization's use of data and information and whether such use is responsible and in their best interests.

- Does your organization have an office or function dedicated to privacy? Compliance?
- Does your organization's privacy and/or compliance function report directly to an independent body in the organization (e.g., Board of Directors)?
- Does your organization have committees at various levels of the organization that set, direct and implement information security and privacy strategy, policy and initiatives?
- Does your organization have a committee that includes senior leaders who are accountable for administrative, technical and physical privacy and information security safeguards?
- Does your organization have a committee responsible for creating privacy and information security policies?
- Does your organization have policies that document accountability for each of the committees/working groups?
- Does your organization have assigned representatives within each of its business functions to assist with the implementation of privacy, information security and compliance policies and procedures?





Policies, Procedures and Guidelines

A comprehensive data governance program that is reasonably designed to protect the security, confidentiality and integrity of sensitive information must be premised, at least in part, upon documented policies, procedures and guidelines which set forth clear standards across the organization and for customers as appropriate. Policies, procedures and guidelines should be examined periodically—at least annually—to maintain their relevance in light of changing legal and operational circumstances.

- Does your organization have published privacy principles or a published privacy policy?
- Does your organization have policies, procedures and guidelines that address compliance with privacy and information security laws and/or regulations?
- Does your organization have Web site privacy policies for its Web sites?
- Are consumer-facing Web sites certified by TRUSTe or the Better Business Bureau?
- Does your organization have policies that govern data access?
- Does your organization have policies that govern data protection?
- Does your organization have policies that govern data transfer?
- Does your organization have policies that govern data transport?
- Does your organization have policies that govern data restriction?
- Does your organization have policies that govern data retention?
- Does your organization have policies that govern data deletion and destruction?
- Does your organization have policies that govern data classification?
- Does your organization have policies that govern breach response and notification?
- Does your organization have a policy on incident response?
- Does your organization require its employees to adhere to a code of conduct?



Audit and Compliance

Meaningful audit and compliance are critical complements to an effective system of data governance policies, procedures and guidelines. The purposes of these audits may be varied, but they are all designed to test against implemented policies, procedures, guidelines, regulatory and legal requirements to ensure that they are working effectively and being adhered to by employees at all levels of the organization and customers/vendors/consumers, as appropriate. They may also be helpful in revealing potential issues, establishing benchmarks and assessing overall privacy and security safeguards, among other things.

- Does your organization have a written annual audit plan and methodology?
- Does your organization conduct audits to verify compliance with your organization's policies and procedures?
- Are audits conducted regularly on all policies? How often? At least annually?
- Does your organization review, audit and update its online privacy policies? How often?
- What is your organization's sampling methodology? Is it 95/5? If not, what is it?
 - Under the 95/5 audit methodology, an annual audit goal is developed such that the random audit sample size contains a sufficient sample to achieve an overall 95% confidence level with a 5% margin of error based on the total population.
- Does your organization's audit plan include audits of customers, employees, vendors and consumers?
- Does your organization conduct audits to ensure compliance with federal and state laws and regulations?
- Does your organization undergo third-party audits by outside accredited third parties? How many per year? What types (e.g., SAS70)?
 - SAS 70 is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
- Does your organization annually review and update its compliance program?

>> Physical Security

Strong physical security controls are one component of an organization's holistic framework that helps ensure the protection of sensitive information maintained by an organization. This includes data on portable devices that should be appropriately secured when outside the physical perimeter of the organization.

- Does your organization have appropriate physical security controls to safeguard data?
- Does your organization monitor employee access to buildings?
- Does your organization require escorting of visitors?
- Does your organization have physical security policies that require employees and contractors maintain a "clean desk" to protect exposure of sensitive data?
- Does your organization have policies and procedures designed to help protect property and assets from unauthorized acquisition, loss or damage?
- Does your organization restrict access to removable and mobile media for employees?
- Does your organization require all laptops to be encrypted?





Technology Solutions

Organizations should use technology solutions, where appropriate, to help safeguard their information and effectively implement their policies and procedures. While people security (employee hiring, training, awareness) and process maturity (automation of key tasks, checks and balances, segregation of duties) are important, technology helps enable the organization by automating key tasks, enhancing manually performed functions and helping prevent malicious access to PII and SPII. Rather than implement a hodge-podge of technology solutions, organizations should adopt a risk-based approach based to their information security framework to decide on the appropriate technology controls that will help minimize risk to PII and SPII.

- Does your organization utilize technology enhancements to aid in network security?
- Does your organization monitor access to sensitive information?
- Does your organization utilize technologies such as encryption and data classification to protect sensitive information?
- Are all databases and other data repositories containing sensitive information, including all organizational servers, secured behind firewalls?
- Does your organization run anti-virus software, and does it have a minimum compliance level of more than 95% at any given time?
- Does your organization run at least weekly vulnerability scans of your critical infrastructure and have strict requirements on addressing issues found?
- Does your organization have an independent network security assessment performed at least annually?
- Does your organization maintain a patch management program that is designed to address desktop and server patches within days of patch release?
- Does your organization maintain technical standards for system setup and configuration and assess a sample of systems against these standards every month?
- Does your organization prohibit employee access to certain categories of Web sites?
- Is your organization compliant with the Payment Card Industry standards for credit card data protection?
 - The PCI Security Standards Council is an independent body formed to develop, enhance, disseminate and assist with implementation of security standards for payment account security.
- Does your organization assess employee passwords for strength at least quarterly, and force password changes on weak accounts?
- Does your organization implement intrusion detection systems at your Internet perimeter, and monitor these devices 24/7 for malicious activity?
- Does your organization have an established Web vulnerability assessment program that focuses on finding and eliminating risks with Web-based applications?
- Does your organization have tools and processes that help automate the user identity management lifecycle (e.g., removing access immediately on employee termination)?
- Does your organization ask employees a secret security question in the event they are locked out of their computers?



Training, Education and Outreach

Training, education and outreach are essential elements for the success of any organization's privacy and information security framework. Internal and external communications programs ensure that all constituencies (employees, customers, shareholders, vendors, consumers, advocacy groups) are aware of the framework's components and responsibilities that accompany those components.

Mandatory training on a regular (suggested annual) basis will help keep privacy and information security top of mind for employees. Additionally, regular privacy and information security reminders and alerts keep employees abreast of current and emerging trends and risks related to privacy and information security. Lastly, outreach to external audiences educates customers, consumers, stakeholders, advocacy communities and others on the good practices of your organization and creates transparency that fosters communication and trust.

- Does your organization have a program for internal and external outreach and communication regarding privacy and information security?
- Does your organization require that employees dedicated to privacy and security obtain appropriate certifications (e.g., IAPP /CIPP, CISM)?
 - International Association of Privacy Professionals/Certified Information Privacy Professional, Certified Information Security Manager
- Does your organization require annual mandatory training for all employees on privacy?
- Does your organization require annual mandatory training for all employees on information security?
- Does your organization require annual mandatory training for all employees on code of conduct?
- Does your organization require annual mandatory training for record retention and deletion?
- Are employees required to pass each training program with a certain percentage of questions answered correctly?
- Are there consequences for not successfully completing training?
- Are privacy and information security policies communicated to employees on a regular basis? How?
- Does your organization send out regular privacy reminders to its employees?
- Does your organization have a program to notify stakeholders on key privacy and information security programs and enhancements?
- Does your organization have hotlines for employees, customers and consumers to report suspicious behavior? What are they?
- Does your organization have liaisons with regulators? Law enforcement? Privacy advocates? Please describe.



Transparency with Consumers

Organizations that are able to enhance interaction with consumers through transparency and accessibility—while effectively communicating the organization's value proposition—will reap the benefits of increased consumer trust and confidence.

- Does your organization have a consumer advocacy office that enhances interaction with consumers?
- Do customers and consumers have easy access to your organization through consumer-friendly and/or dedicated Web sites?
- Do consumers have the ability to request certain information available about them? Is there a cost to obtain this information?
- Does your organization provide a vehicle for correction should a consumer wish to dispute the accuracy of information contained in a report?
- Does your organization provide easily accessible tools (e.g., a video, Web site) to answer questions and explain the benefits that consumers receive as a result of your organization's services?

