PRIVACY/ CONFIDENTIALITY

Privacy and confidentiality are two critical IT security concepts – it is important to understand what they mean; how they are related; and how to implement controls to protect data from unauthorized release.

Confidentiality is defined as the means to protect personal, sensitive or proprietary information from disclosure. The National Institute of Standards and Technology (NIST) define confidentiality as:

> *"preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."*

Webster Dictionary defines ***privacy*** as 'the quality or state of being apart from company or observation; freedom from unauthorized intrusion." The boundaries and content of what is considered private differ among cultures and individuals. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps security (confidentiality) including the concepts of appropriate use and protection of information. Privacy is often discussed as a basic human right. Deciding what to share with others is your specific right, however, rules govern how businesses collect and use personal information as it relates to privacy statues.

As a business owner, your employees and customers have an expectation that your organization will protect their private/personal information. If you maintain a web presence, you were required to publish a privacy policy. In the privacy policy, your organization was required to disclose the information collected via the web and how the organization uses the information.

FACT 1: PRIVACY 101

The Fourth Amendment of the Constitution provides an implicit right to privacy through protections against "unreasonable searches and seizures". In 1890, the Supreme Court defined privacy as "the right to be let alone" or freedom from inference and intrusion. Prior to the advent of the Internet, privacy concerns focused on intrusions by government and/or law enforcement.

DID YOU KNOW…

- ✓ Privacy:
  - Consumers decide what to share
  - If you collect it, know what it means to hold it and for how long
- ✓ Privacy Impact Assessment – do I need one? YES!
- ✓ Privacy Policy – is a summary of how PII data will be used, stored and maintained – can include both digital and paper records
- ✓ States also have their own privacy laws in addition to federal laws
- ✓ If you violate your privacy policy, your business could be held liable
- ✓ Confidentiality is the means to protect sensitive data

Still have questions, need help?
Contact us at our **"Ask-an-Expert"** service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

PRIVACY/CONFIDENTIALITY continued….

FACT 2: U.S. PRIVACY LAWS

Legislation in the United States concerning data privacy is largely sector based, meaning that each law or regulation has been created in response to the needs of a particular industry or section of the population. Examples include: Children's Online Privacy Protection Act, Health Insurance Portability and Accountability Act, Video Protection Privacy Act, Gramm-Leach-Bliley Act. The Federal Trade Commission Act (15 U.S.C. Sec 41-58) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies.

For a more detailed review of U.S. privacy laws, visit Reuters Practical Law, Data Protection in the U.S., Overview, by Leuan Jolly, July 2017.

The National Conference of State Legislators (NCSL) maintains a list of state data security and privacy laws and also pending legislation. See http://www.ncsl.org/

FACT 2: PRIVACY IMPACT ASSESSMENT (PIA)

A Privacy Impact Assessment is an analysis of how personally protected information (PII) is collected, used, shared and maintained. It is the first step in developing a privacy policy for your business. As a business, you are required to protect PII that you collect on your suppliers, customers, partners and/or employees. PII is any data that could potentially identify a specific individual – ***information that can be used to distinguish one person from another.*** PII is categorized as either sensitive or non-sensitive.

Non-sensitive PII is any data that is publically available – in the phone book, public records – it is data that can be transmitted and stored unencrypted. This is data that if released will not result in harm to an individual. Examples include business addresses, business emails, and business telephone numbers.

Sensitive PII is data that is unique to the individual – that if combined with non-sensitive data can distinguish one person over another. Social security numbers, passport numbers, genetic/genomic test data.

The first step in conducting a PIA is to identity the systems and/or processes that collect PII data. Another approach is to identify the personas that your business interacts with and the PII collected and used as part of the business process. An example would be a website – who are the people that interact with your site and what interactions are involved? Customers, employers, suppliers and/or the general public could have different experiences. Understanding how these personas interacts with your business and the data collected through each transaction is important to the PIA.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

PRIVACY/CONFIDENTIALITY continued….

A good tip to conduct this analysis is to build a spreadsheet:

1) Identify the persona;
2) Identity what data is collect with each persona and transaction to include PII;
3) Describe how the data is used (date would be helpful);
4) Describe how it is stored (PII should be encrypted);
5) Define the measures taken to protect the data from disclosure and unauthorized access.

Review and update annually.

FACT 3: PRIVACY POLICY

A Privacy Policy is a legal document that describes how your business collects, uses and maintains data it collects from its customers, suppliers, employees and the general public. If your business does a thorough job in completing a PIA, the policy should be the narrative that compliments the analysis. As a legal document, your business will be held responsible to the statements made in the document, especially in terms of ***appropriate use***. As an example, "***appropriate use"*** in terms of collecting customer emails and physical addresses could be stated that it is being used to send periodic notifications to ***your*** customers. Inappropriate use of customer emails would be selling or sharing customer emails to third party suppliers without their users knowledge and consent. The FTC has issued several consent decrees to businesses for violating their stated privacy policy and sharing customer data inappropriately.

FACT 4: CONSUMER PRIVACY

What does privacy mean to me, as a consumer? Data privacy focuses on the use and control of personal data, such as rules that safeguard consumer's personal information. Consumer privacy is focused on the legal and political issues and the public's expectation of privacy with the collection and dissemination of data by businesses and merchants. Consumers are becoming more and more cognizant of the collection, use and handling of their data based upon the numerous data breaches that have occurred in the past five years.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

PRIVACY/CONFIDENTIALITY continued….

FACT 5: CONFIDENTIALITY

Simply put, confidentiality is the requirement that private or personal information not be disclosed to, and hidden from, unapproved people within the organization. Confidentiality is one of the three triads in information security – the others are integrity and availability. Confidentiality revolves around the idea of "least privilege", access to information should be granted only on a need-to-know basis so information that is only available to some should not be accessible by everyone. Confidentiality protections are the controls established to protect PII and are defined in the organization's privacy and security policies.

- NIST treats the loss of confidentiality as the unauthorized disclosure of information
- Confidentiality protection applies to data in storage, during processing, and while in transit
- For example, encryption processes support confidentiality since it protects sensitive information from theft or leakage by converting plain text into hidden text
- Good confidentiality comes from a strong data classification policy, without classifying information it will be difficult to maintain who has access to what, and how to implement controls.

FACT 3: RESOURCES/REFERENCES:

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
https://www.law.cornell.edu/uscode/text/44/3552
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf
http://resources.infosecinstitute.com/cia-triad/#gref
http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf
http://resources.infosecinstitute.com/cia-triad/#gref
https://www.law.cornell.edu/constitution/fourth_amendment
http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf
https://iapp.org/about/what-is-privacy/

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.