SECURITY INDUSTRY ASSOCIATION

Data Privacy Code of Practice Access Control

Produced with support from:

SONICWALL®

SECURITY INDUSTRY ASSOCIATION

securityindustry.org

INTRODUCTION

There has always been a need in society to ensure that only the "right" people can enter restricted areas. Like other aspects of security, what once was a manual operation is now largely conducted through the use of technology. Solutions that provide access control and identity management keep people, property and information safe in all types of areas around the world, from office buildings to critical infrastructure to military sites and other locations vital to national security and social stability.

These technological approaches necessarily require the collection of sensitive data about individuals, including personally identifiable information (PII), such as names, birth dates and addresses; employment status; and biometric identifiers from faces, fingerprints, irises or other features. Leveraging data points through technology enables a high degree of security (that is scalable to the needs of the site), efficient throughput at entry points and reduced demand on personnel. Collecting and holding this information, though, creates a new kind of risk – specifically, unauthorized release of or access to the data – and a resulting need for measures to mitigate it.

Breaches, insider threats and unintentional leakages are just a few of the risks related to sensitive information, and any one of them can inflict severe damage both on the person whose data is disclosed without authorization and on the organization that was entrusted with that data. The Security Industry Association (SIA) Data Privacy Advisory Board has produced this Code of Practice for Access Control ("Code") based on common privacy and security principles to provide manufacturers, integrators and end users with guidance that can be used to inform their development of sound policies and practices that mitigate privacy risks while leveraging the power of access control and identity management technology.

AREAS OF RESPONSIBILITY

Manufacturers

Manufacturers of access control solutions are generally well removed from the data handling process. By producing the tools that enable digital collection and analysis, though, they bear certain responsibilities, primarily related to device and platform default configurations and upkeep, as well as the building of privacy into the design of hardware and software. The factors below extend from the product design phase through its in-service lifespan.

- Role-based access control, multi-factor authentication, encryption and other data security best practices built in (privacy by design)
- Forced changing of default login credentials
- Publicly available and current guidance to secure infrastructure
- Communication of identified vulnerabilities
- Patching
- Device security risk considerations and notifications (e.g., trusted platform details)
- Cloud services security and management, if apps are offered

Integrators

Integrators deploy the systems that make access control and identity management possible. This creates a special responsibility for them to set the end user up for success. Conducting a privacy impact assessment can identify areas of concern before installation begins. Other important areas for integrators to consider include:

- Privacy principles built into the system (privacy by design)
- Requirements, roles and responsibilities, including third-party security
- Nature of systems involved (cloud, on premises, hybrid) and designated privacy and security measures
- Ongoing privacy and cybersecurity education and training for employees
- A service contract that identifies the integrator’s privacy and security obligations and risk
- Applicable international, federal, state, and local laws and regulations, as well as industry standards, frameworks and best practices (note that the use of biometrics may produce additional compliance requirements)

End Users

End users, in privacy terms, are the data controllers. They establish the purpose and justification for the access control and identity management system as well as its operational scope.

As a rule, then, it is the legal and ethical responsibility of end users to ensure that the system complies with laws and regulations and adheres to industry best practices. This starts with conducting a privacy impact assessment (possibly in collaboration with their integrator) to identify what and how data is collected, used, shared and stored – as well as the related vulnerabilities and threats – and to start planning risk mitigation measures. These measures start with the implementation of foundational data handling principles, including:

- Purpose limitation: Identify the specific reason for collecting personal information and the justification for doing so
- Notification and consent: Ensure that people who are enrolled in the system are made aware of how their information will be used and provide (preferably written) consent (which should be revocable if an individual changes his or her mind)
- Data minimization: Collect only the information that is necessary to carry out the identified purpose and keep the data only for as long as it is needed
- Data accuracy: Verify that the collected data is correct to ensure fair treatment of individuals and proper functioning of the system
- Security: Encrypt personal data at an appropriate level while it is at rest, in transit and in use. Remember the information security principles of the CIA Triad – Confidentiality, Integrity, Availability
- Access limitation: Adopt the "principle of least privilege"; that is, allow only vetted people with a legitimate need to have access to sensitive data; day and time limitations on access may also be appropriate
- Assessments and audits: Vulnerability assessments can reduce the risk of attacks from outside the organization, while auditing data access records can mitigate insider threats by identifying if inappropriate/unusual/unauthorized access has occurred
- Response plan: Have a plan in place in the event of a breach or other leakage of sensitive information

End users should provide all members of their organization with training on privacy issues. Those who have access to sensitive data should receive more thorough training to ensure full understanding of the principles listed above.

In addition, when hiring a third-party services provider, the end user should take reasonable steps to ensure that the provider handles data with an adequate level of care. The end user retains the ultimate responsibility to protect data and respect privacy and should not solely rely on other entities for compliance.

LEGAL CONSIDERATIONS

The United States does not have a national privacy law, but at least 19 states have broad privacy requirements, according to the International Association of Privacy Professionals, with the California Consumer Privacy Act (and its successor, the California Privacy Rights Act) the best known and most far-reaching state law. All states have laws related to breach notification.

Some features common across state privacy laws include consumer rights to access, deletion (under certain circumstances), and portability of data (that is, the ability to easily transfer or move data between different systems, applications or platforms), as well as the right to opt out of data sales. Notwithstanding some similarities, though, privacy laws vary widely, creating compliance challenges for organizations that conduct business across state lines.

In recent years, privacy has been a frequent topic of discussion in Congress, though no proposal has passed both the House and the Senate. Negotiations typically break down over disagreements regarding whether to include two provisions: preemption (the federal law would supersede all state laws) and private right of action (individuals would be able to file lawsuits in response to privacy violations).

Internationally, the General Data Protection Regulation establishes strict rules for the handling of personal information in the European Union. It is important to note that there are circumstances in which non-EU organizations can fall under the law’s jurisdiction.

Privacy compliance, clearly, can be a complicated topic, one that grows more complex as an organization conducts business in more states and more countries. It is essential to have legal counsel review an organization’s data handling practices and privacy policies to ensure that they meet applicable legal requirements.

SELECTED GLOSSARY

Biometrics – the use of an individual's physical features (e.g., face, iris, fingerprint) by a device to confirm identity

CIA Triad – A mnemonic referring to three key components of information security: Confidentiality (protecting data in all of its phases – at rest, in transit, in use); Integrity (preventing data from being altered or otherwise corrupted); Availability (ensuring that authorized users can access the data when it is needed)

Data controller –The entity that determines the purposes for which, and the means by which, personal data is collected and processed and the related policies; for the purposes of this Code, the end user typically is the data controller

Multi-factor authentication (MFA) – A secure access approach that allows a user entrance to a website, application or facility only after they have presented two or more pieces of evidence to prove they are who they say they are; this typically includes something they know (such as a password), something they have (such as a token), and/or something they are (such as a fingerprint)

Patching – A change to a computer program or its supporting data that updates, fixes or improves the program, often by addressing an identified vulnerability

Personally identifiable information (PII) – Information that can be used to identify an individual, either by itself or when combined with other information

Privacy by design – An approach to privacy that integrates privacy principles into the core of product and system development; it emphasizes the importance of designing systems with privacy as a default setting, incorporating privacy considerations from the initial stages of development, and viewing privacy as a right

Privacy impact assessment – A tool that can be used to gauge risk by examining the way information is collected, used, shared, maintained and retained and that identifies operational requirements and risks; one should take special note of the impact of integrating access control and identity management systems with video surveillance systems

SIA DATA PRIVACY ADVISORY BOARD

The SIA Data Privacy Advisory Board provides information and best practices to help SIA members handle sensitive data in a safe and secure manner to protect the personally identifiable information of their employees, partners and customers from potential breaches. The board leverages the collective expertise of industry professionals, law enforcement, security practitioners and data privacy experts to inform and educate SIA member companies about methods for mitigating the risk of data breaches.

SONICWALL® SIA thanks SonicWall for its support of this project.

Disclaimer: The information provided in this Code does not, and is not intended to, constitute legal advice. All information is for general informational purposes only. Readers of this Code should contact their attorney to obtain advice with respect to particular legal matters. No reader of this Code should act or refrain from acting on the basis of the information in this Code without first seeking legal advice from counsel in the relevant jurisdiction. The content of this Code is provided "as is"; no representations are made that the content is error-free.

securityindustry.org