Data Security Best Practices

The Consumer Protection Section[1] of the Colorado Department of Law, led by the Attorney General, is responsible for enforcing data security laws that apply to private entities and government agencies. Covered entities that maintain protected personal or personally identifying information (PII) must take reasonable steps to protect that information, to dispose of it when it is no longer needed, and to promptly notify Colorado residents when their information is at risk of misuse by unauthorized third parties.[2] Another law, the Colorado Privacy Act, also requires covered entities to implement appropriate technical and organizational data security safeguards.[3] Colorado data security laws and the Colorado Privacy Act are codified within the Colorado Consumer Protection Act and the Colorado consumer code.[4]

While each entity's data security needs and practices may differ, there are some common best practices that most, if not all covered entities can implement. Thoughtful data security practices can help limit data breach risk, potential harm to victims in the event of a data breach, and an entity's expenses in responding to a data breach.

[1] The Office of the Attorney General, Consumer Protection, https://coag.gov/office-sections/consumer-protection/.
[2] C.R.S. §§ 6-1-713, 713.5, 716; §§ 24-73-101, 102, 103.
[3] C.R.S. §§ 6-1-1305(4), (5).
[4] C.R.S. §§ 6-1-101-1313.

Key Steps to Protecting your Data

This guidance document is based on the Attorney General's data security cases[5] and relevant Colorado statutes.[6] It should be noted that implementing the practices outlined in this document alone may not be sufficient for an entity to be fully compliant with Colorado law.

#1 Inventory the types of data collected and establish a system for how to store and manage that data.

In order to identify proper data security measures, an entity should first identify the types of data it collects and stores and note the source and purpose of the data as well as which employees have access to that data. An entity, for example, may store its employees' Social Security numbers on a hard drive or customer contact information in cloud storage and limit access to only human resources or sales employees. Any such entity should develop written data retention and destruction policies to ensure that PII is properly disposed of when no longer needed.[7] The policies should also set limits on how long personal data will be held and create procedures to limit non-secure storage of personal data, including providing for the deletion of any sent or received emails that contain PII.

5] For information on how and when the Attorney General's Office has enforced non-compliance with these laws visit: https://coag.gov/office-sections/consumer-protection/consumer-protection-cases/.
[6] The Office of the Attorney General, Data Protection Laws, https://coag.gov/resources/data-protection-laws.
[1] See SEMA Construction Assurance of Discontinuance, https://coag.gov/app/uploads/2021/11/SEMA-Construction-Fully-Executed-Assurance-of-Discontinuance.pdf (enforcement action against a company for failure to maintain reasonable security practices including a reasonable data destruction policy and timely notify Coloradans of a data breach).

#2 Develop a written information security policy.

An information security policy should include procedures related to common security practices such as data minimization, access control, password management, and encryption. The policy should also follow information security standards relevant to the type of information the entity seeks to protect.[8] For example, entities that collect credit card information must protect that information in accordance with the Payment Card Industry's Data Security Standard, entities that store employee information should consult ISO/IEC 27000 standards, and small businesses that are creating a security program might look to CIS Controls to determine their priorities. Measures the entity takes to comply with any appropriate standard should be reflected in the policy. The policy should also be easily accessible, and employees should be aware of the policy and be trained appropriately to ensure compliance.

#3 Adopt a written data incident response plan.

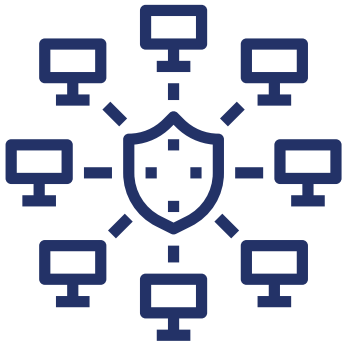
An incident response plan should detail the steps an entity will take in the event of a data incident. By developing and implementing such a plan, companies will be better positioned to take remedial action and notify consumers and the Department of Law in a timely manner if PII is at risk of being misused. A copy of the plan should be kept in paper form should a cyberattack render computerized systems unusable. An entity should conduct employee incident response training and practice its incident response plan through table-top exercises.

[8] See Impact Mobile Home Communities Assurance of Discontinuance, https://coag.gov/app/uploads/2021/06/AOD-Signed-Impact-MHC-and-Colorado-6.11.2021.pdf (enforcement action against a company for failure to maintain reasonable security practices including employee cybersecurity preparedness training and timely notify Coloradans of a data breach).

#4 Manage the security of vendors.

Recognizing the reality that networks are interconnected, entities should carefully vet potential vendors to ensure they implement necessary security practices and negotiate terms[8] in vendor contracts to require appropriate security measures, including regular audits. Colorado's security breach notification law requires service providers to aid covered entities in the event of a security breach.[9] The new Colorado Privacy Act will require data security related contractual obligations between entities and vendors who process personal information.[10]

#5 Train your employees to prevent and respond to cybersecurity incidents.



Entities should train employees on cybersecurity preparedness and foster a sense of collective responsibility for data security.[11] Training employees to identify and report phishing emails and other suspicious network activity is particularly important in preventing cyberattacks and protecting Colorado residents.

[9] C.R.S. § 6-1-716(2)(b).
[10] C.R.S. § 6-1-1305.
[11] See Impact Mobile Home Communities Assurance of Discontinuance, https://coag.gov/app/uploads/2021/06/AOD-Signed-Impact-MHC-and-Colorado-6.11.2021.pdf (enforcement action against a company for failure to maintain reasonable security practices including employee cybersecurity preparedness training and timely notify Coloradans of a data breach).

#6 Follow the Department of Law's ransomware guidance to improve your cybersecurity and resilience against ransomware and other attacks.

A ransomware attack that compromises personal information may constitute a data breach under Colorado law.[12] Companies should be equipped to access backup copies of their files in the case that a ransomware attack renders a system encrypted and inaccessible. You can find the Department of Law's ransomware guidance by clicking here.[13]

#7 Timely notify victims and the Department of Law/Attorney General (when required) in the event of a security breach.

An entity that experiences a potential data security breach (e.g., finds its network has been accessed by an unauthorized actor) should conduct a prompt investigation to determine whether a security breach has occurred.[14] If the entity determines that personal information has been or is likely to be misused, the entity must notify affected Coloradans within 30 days. If the security breach affects 500 or more Coloradans, the entity must also notify the Department of Law within 30 days. A full list of notification requirements may be found here.[15] To notify the Department of Law, reporting entities should use the online reporting tool found here.[16]

[12] See Kozleski CPAs Assurance of Discontinuance, https://coag.gov/app/uploads/2022/01/2020.06.08-KozleskiAssuranceAgreement06082020.pdf (enforcement action against a company for failure to conduct a prompt, good faith investigation after experiencing a ransomware attack).
[13] The Office of the Attorney General, Attorney General Phil Weiser joins fellow AGs in alerting businesses and government entities to take prompt action to protect operations and personal information (July 29, 2021) https://coag.gov/press-releases/7-29-21-2/.
[14] See SEMA Construction, Inc. Assurance of Discontinuance, https://coag.gov/app/uploads/2021/11/SEMA-Construction-Fully-Executed-Assurance-of-Discontinuance.pdf (enforcement action against a company for failure to conduct a prompt, good faith investigation and timely notify victims of a phishing attack).
[15] The Office of the Attorney General, Data Protection Laws, https://coag.gov/resources/data-protection-laws/.
[16] The Office of the Attorney General, Data Breach Notification Report Form, https://coag.gov/data-breach-notification-report-form/.

#8 Protect individuals affected by a data breach from identity theft and other harms.

An entity that collects PI has a duty to be a good data steward. This duty includes compensating and protecting individuals affected by a breach. One way to do this is to timely notify victims of a breach and provide victims access to free credit monitoring services.

#9 Regularly review and update your security policies.

Entities should regularly review their data collection, storage, and use practices for changes to internal processes as well as associated risks. Data retention, security, and incident response policies should be updated to reflect any changes to data collection and storage practices or increased risks to maintaining personal information.