CCPA “REASONABLE SECURITY” CHECKLIST

If your business serves consumers who are California residents, you may be subject to the California Consumer Privacy Act (CCPA)—even if you’re located outside of the state. One of the requirements is that you implement and maintain “reasonable security” to protect certain personal information. Here are 15 steps to getting there from ESET experts.

Know your data
Understand the personal information you have, how it was collected, where it resides, who has access, and for what purpose.

Don’t hoard data you don’t need
If there isn’t a sound business reason to have personal data, get rid of it so you don’t have to protect it.

Appoint a Data Protection Officer
Appoint a single point person for staff training, handling consumer requests, auditing your security, and ensuring compliance with the act.

Control access to data sensibly
Categorize personal data, and enforce a policy that grants access by individuals and devices to those categories based on business need.

Require secure authentication
Require strong, frequently changed passwords, limit login attempts, and implement multi-factor authentication for sensitive-data access.

Don’t store passwords in plain text
Store passwords that are part of customer data in hashed form or even better, hashed and salted, to stop anyone with access from being able to see the actual password.

Store and transmit securely
Deploy an endpoint encryption solution that manages encryption keys remotely, and enforces policy for files, drives, drives, memory sticks and emails.

Segment and monitor the network
Place sensitive data on separate servers, protect them with additional firewalls or other security measures, and monitor who attempts access.

Secure remote access and endpoints
Require VPN access and strong 2FA, and extend endpoint protection to cover remote access as well as all endpoints, servers and mobile devices.

Develop for security
Make sure your customer-facing services are built with a “secure by design” development ethic, and have them tested them for security.

Ensure third-party security
Build security requirements into your agreements with service providers, and ensure their security policies match or go beyond your own.

Keep your protection current
Stay current with software patches and test infrastructure, products and services on a regular basis for vulnerabilities.

Test backup and recovery
Put a process in place for regularly testing, assessing and evaluating the effectiveness of your measures.

Promote cybersecurity awareness
Promote awareness of the need to protect consumer data companywide, and provide regular training on data protection and cybersecurity.

Secure the physical realm
Secure entryways to areas that house personal data, protect laptops and drives from theft, and shred documents with personal information.

How ESET can help

Endpoint Protection

Protects against data breaches, ransomware, targeted attacks, fileless malware and advanced persistent threats, and blocks network-level vulnerabilities that can spread malware.

Endpoint Encryption

Makes encryption easy for end-users, enforces security policy for files on hard drives, portable devices and emails, and supports full-disk encryption.

Multi-Factor Authentication

Is a simple, effective way for businesses of all sizes to implement multi-factor authentication.

Cybersecurity Awareness Training

Keeps employees focused with interactive methods, delivering training that truly changes behavior—for free.

Data Loss Prevention

From Safetica covers all data leak channels, and identifies suspicious activity that could lead to a data breach.

Backup and Recovery

From Xopero covers your entire environment and protects business data no matter where it is stored.

To learn more about CCPA, how it may impact your current cybersecurity profile and what steps to take next, or to explore ESET solutions, visit: eset.com/us/ccpa

Disclaimer

This checklist is a general overview of the CCPA only, and is not intended as legal advice. The document reflects the act as understood as of the date of publication. For legal advice and your compliance, contact a qualified attorney.

ENJOY SAFER TECHNOLOGY™

AUTHORS:
Tony Anscombe, Lysa Myers and other ESET experts // August 2019