Information Security Practices

Protecting Customer Data

ca technologies

A message to our Customers/ A message from our Chief Information Security Officer

CA Technologies recently celebrated its 40th birthday. Few technology companies have had the good fortune of making it through a decade, let alone four, and for that we thank our customers for continuing to put their business and trust in CA. It is a responsibility we do not take lightly, and one we have embedded in every aspect of our culture. Just this year, our CEO Mike Gregoire rolled out a new culture Mission that is entirely focused on you, your experience with CA, and your goals. When you win, we win.

In the era of the Application Economy, your data has become more than just a part of your business, it has become the cornerstone, and one that is constantly under attack. Every day we hear about a cybersecurity breach, hack, or troubling misuse of information. Taking measures to protect and secure your data is something CA has done for years, but we want our customers to know and understand how robust our practices are. CA is fully committed to protecting your data and information as if it were our own.

Our information security program is a holistic approach that considers every aspect of how we may store, collect, access, or touch your data. From engineering to finance, every person at CA plays a role. This document outlines the policies, procedures, and physical and technical safeguards we have implemented to achieve this. We are proud of what we do, but we are always working to make it better, faster, and more secure. As always, we thank you for our business, and look forward to another 40+ years of being the technology company you trust.

Securely Yours,

David Billeter

Chief Information Security Officer (CISO)

I. SECURITY BY DESIGN

a. Secure Code Development

All CA developers are required to follow CA's Product Securability Policy and Procedure which provides for securability standards, strategies, and tactics for each phase of the product development lifecycle informed and consistent with industry best practices. The procedure requires product classification based on risk rankings determined by use cases, application of static code analysis tools, and penetration testing.

b. Secure Code Release

Prior to release of any product to CA's Customers, antivirus/antimalware scanning is performed, and based on the risk profile additional penetration testing may be performed. Any identified vulnerabilities are tracked in the central CA defect tracking system together with an associated risk rating and are not approved by the Securability Center of Excellence unless remediated. Vulnerabilities are ranked using the Common Vulnerability Scoring System (CVSS) in accordance with the NIST Framework to determine their severity and response.

II. HOW A CUSTOMER'S DATA COMES INTO CA AND ITS PROTECTION

a. Access to Customer Data

CA may obtain Customer data in a number of ways, including, through a support ticket, services engagements, or the use of a CA SaaS offering. All files submitted by our customers, regardless of how acquired, is categorized as "Highly Confidential Data" requiring the highest degree of protection. In the event CA's professional services team is required to be at a Customers' facility, such individuals are prohibited from downloading any Customer data to their devices and removing them from the Customer's facility.

b. Physical Security

CA maintains and administers the following physical access controls:

- Employees and contractors are subject to background checks prior to being offered employment or given access to CA's facilities and systems.

- All facilities require badge access for employees and contractors and intrusion detection alarms at ingress and egress points. Visitor access must be logged in a physical access log and visitors are escorted through restricted areas in the facility.

- All data centers where Customer data is processed or stored are further protected by security guards and monitoring cameras (e.g., CCTVs) 24/7.

c. CA Authorized User Names, Passwords and Authentication

CA monitors access rights to ensure access adheres to the least privilege principle commensurate with the CA's user's job responsibilities, logs all access and security events, and uses software that enables rapid analysis of user activities.

CA's passwords are administered in the following manner:

- Passwords are communicated separately from user IDs
- Passwords are not shared
- Initial password generation is random
- Initial password change is required
- Passwords must have minimum length and complexity and must be changed on a regular interval without reuse of recent previous passwords
- CA passwords are encrypted and passwords are never recoverable and can only be securely reset.

III. Enterprise Role-Based Access

The logical access procedures define the request, approval, access provisioning and de-provisioning processes. The logical access procedures restrict user access (local or remote) based on user job function for applications and databases (role/profile based appropriate access) for applications, databases and systems to ensure segregation of duties and are reviewed, administered, and documented based on on-boarding, resource re-assignment or separation. User access reviews are performed to ensure access is appropriate throughout the year.

All CA system administrators are authenticated using multi-factor authentication for system access through privileged access management. In addition, the use of privileged access management enables all system admin sessions and console access to be recorded and CA records all such sessions and access for audit and forensic purposes.

For Customer data entered via a CA SaaS Offering, CA database administrators (DBAs) may be required to access Customer data in the course of various technical operations. Default DBA accounts in the database are expired and locked except when the account is required to be used by the DBA to complete their job. Database access is granted upon formal authorization through a ticket and access is granted only to authorized personnel based on job responsibilities registered in an Active Directory. Where it is not feasible to lock the DBA account, passwords are changed for each access request. All database accesses are logged. Employees' user access accounts are reviewed on a quarterly basis. Access account reports are generated by a Security Analyst and sent to managers for review and approval. This review and approval are documented in a CA support ticket where any discrepancies and resolutions, if any are listed.

IV. HOW IS DATA TRANSMITTED? NETWORK SECURITY MANAGEMENT

a. Network Controls

CA utilizes firewalls for access control between CA's networks and the Internet. Firewall access is restricted to a small set of super users/administrators with appropriate approvals. Firewalls are established with minimum rights necessary to accomplish tasks by role and access is authorized on a "deny by default" policy.

Periodic network vulnerability scans are performed and any critical vulnerabilities identified are promptly remediated. In addition, penetration tests are also performed by security professionals, both CA employees and third parties.

b. Network/Communication Security Policy/Encryption

Defined Access Control Lists (ACLs) to restrict traffic on routers and/or firewalls are reviewed and approved by network administrators. IP addresses in the ACLs are specific and anonymous connections are prohibited.

Customer data is encrypted while in transit over any public network or wireless network (wireless networks are not used in SaaS Offerings) via CA's Secure File Transfer Protocol (SFTP) to transmit flat files.

CA utilizes an information protection and control solution that is designed and administered to minimize the accidental, negligent and malicious misuse of data through email and other communications aimed outside of CA's firewalls (*e.g.*, a data loss prevention (DLP) solution).

[remainder of page intentionally left blank]

c. Remote Access Administration

The following remote access settings are applicable:

- Unauthorized remote connections from devices (e.g., modems) are disabled as part of standard configuration.
- The data flow in the remote connection is encrypted and multi-factor authentication is utilized during the login process.
- Remote connection settings limit the ability of remote users to access both initiating network and remote network simultaneously (no split tunneling).

d. Third Party Remote Access

Dependent third party service provider (i.e., subcontractor) remote access adheres to the same or similar controls, and any subcontractor remote access has valid business justification.

e. Removable Media

Removable media is not in use for the delivery of CA Technologies SaaS offerings. In addition, all laptops and other removable media on which Customer data is stored, such as backup tapes, are encrypted.

V. AUDITS OF CONTROLS AND CERTIFICATIONS

The respective audit criteria (e.g., PCI, SSAE 16 SOC 1, TYPE 2) followed by third party auditors inspecting CA's security practices with regard to SaaS offerings along with summary reports of the auditors can be found at: http://www.ca.com/us/lpg/saas-summary-audit-report.aspx. In addition, CA's internal data centers, those which may house Customer data received through support or services interactions, are ISO/IEC 20000 for IT service management and ISO/IEC 27001 for security controls certified.

VI. SECURITY INCIDENTS

CA maintains a highly confidential cybersecurity Incident Response Plan designed to identify, categorize, remove, and remediate cybersecurity incidents. The Plan is reviewed bi-monthly with annual tabletop exercises. The mission of the CA Technologies Cybersecurity Operations is to prepare the organization to identify and respond to information security threats and incidents while containing and restoring normal service operations as quickly and effectively as possible.

In the event CA discovers a security incident, CA has the following target response and remediation time lines:

Severity Level	Description	Examples	Target Response	Target Remediation/ Escalation
1	Incidents that have a severe impact on CA Technologies or its customers' business or services	• Malicious code attacks • Unauthorized access • Denial of Service (DoS) affecting an entire campus • Compromise of host with sensitive data, including Sensitive Personal Data	1 Hour	2 Hours
2	Incidents that have a significant impact, or the potential to have a severe impact on CA Technologies or its customers' business or services	• Attempts to gain unauthorized access • DOS attack affecting a building or department • Open mail relay	4 Hours	1 Business Day
3	Incidents that have a minimal impact with the potential for significant or severe impact on CA Technologies or its customers' business or services	• Unauthorized network probes or system scans • Isolated virus infections	1 Business Day	2 Business Days
4	Incidents that have a minimal impact with no potential for significant or severe impact on CA Technologies or its customers' business or services	•Improper Usage, •Unauthorized software (non-malicious) •Policy Violations	2+ Business Days	2+ Business Days

VII. COMPLIANCE WITH DATA PRIVACY LAWS

a. CA Technologies' Privacy Statement is posted on our website (www.ca.com/us/privacy), and local websites in other countries, and describes how

CA Technologies uses personally identifiable information that it collects on the website as well as data collected off-line.

b. CA Technologies implements processes designed to ensure that we comply with all applicable data privacy and security laws in the US and in all countries in which we do business, including breach notification laws, state and federal privacy-related legislation, and national laws.

c. CA Technologies has several internal Privacy Policies, including an HR Privacy Policy and a Privacy and Data Protection Policy, which mirrors the EU Data Privacy requirements.

d. CA Technologies also maintains a Policy that specifically addresses the handling of customer data and a Written Information Security Plan (WISP) in compliance with the Massachusetts information security regulations and other US laws.

e. In September of 2016, CA self-certified to the EU-US Privacy Shield framework which was designed by the U.S. Department of Commerce and European Commission to provide global companies with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. In April of 2017, CA self-certified to the Swiss-US Privacy Shield framework. CA's participation in the Privacy Shield means that CA and its U.S. subsidiaries have agreed to comply with the Privacy Shield Framework regarding the collection, use, and retention of EU and Swiss personal data that it uses as a data processor. To learn more about the Privacy Shield Framework, and to view CA's certification page, please visit https://www.privacyshield.gov/.

f. CA Technologies also holds Binding Corporate Rules for Controllers and this is our method for transferring data globally as a data controller http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

g. In addition, CA Technologies has prepared a downloadable data processing agreement (DPA) setting out CA's commitment to privacy and data protection when processing customer data in connection with the provision of products and services to our customers and partners. This DPA also covers with the transfer of personal data outside of the European Economic Area and Switzerland in connection with the provision of such products and services. The DPA can be found at www.ca.com/us/data-transfers.aspx. If you have any questions, please feel free to send an email to datatransfers@ca.com.