Global Information Security

CalAmp®

Information Security Program Overview

September 2021

1.0 Overview 3
2.0 Purpose 3
3.0 Scope 3
4.0 Program Statements 3
4.1 Required Programs 3
4.1.1 Information Security Program Components 4
4.2 Program Procedure Requirements 6
4.3 Exceptions 6
4.4 Policy Distribution 6
4.5 Program Review 7
4.6 Responsibility Assignment 7
4.7 Program Reporting 8
4.8 Security Program Compliance 8
5.0 Additional Considerations for Information Security Program 9
5.1 Organizational Structure 9
5.2 Program Review Maintenance 9
5.3 Cybersecurity Liability Insurance & Incident Response 9

1.0 Overview

CalAmp's shareholders, customers, suppliers, technology partners and employees rely on us to have a comprehensive global information security program to ensure information and data protection, privacy and governance. As a public company that operates in multiple jurisdictions around the globe, we are subject to a wide variety of data protection laws with which the company complies. The following fundamental concepts are crucial to the development, implementation and maintenance of our information security program:

- Confidentiality – The confidentiality of information shall be maintained and monitored.
- Integrity – The integrity and completeness of information shall be assured.
- Availability – Information shall be available for authorized use when and as needed.
- Privacy – Adequate protection of personal/customer/employee/company data shall be assured and monitored.

Cybersecurity Framework – CalAmp leverages the National Institute of Standards and Technology (NIST) Cybersecurity Framework to outline best practices, based on industry standards, to align on and address cyber risk and data privacy.

2.0 Purpose

The following statements establish the overall framework of the information security program and denotes other related policies regarding various facets of the information security and data privacy programs.

3.0 Scope

These program statements are to CalAmp Corp. ("CalAmp" or the "Company") and its subsidiaries, divisions, locations, staff, contractors, temporary workers, suppliers, and any individual or entity who is provided access to our information resources and network. This document is the responsibility of CalAmp executive management and subject to the oversight of the Cybersecurity and Data Privacy Committee of the Board of Directors.

4.0 Program Statements

4.1 Required Programs

Information Security Program – CalAmp will develop and maintain a comprehensive, written information security program to secure all enterprise-wide information assets in a manner commensurate with each asset's value and/or any security or confidentiality requirements with respect to such asset, in each case as established by a global risk assessment and mitigation program.

Data Privacy Program – CalAmp will develop and maintain a comprehensive, written data privacy program that will secure CalAmp employee, customer, vendor and contractor personally identifiable information (PII) against unauthorized use or disclosure.

4.1.1 Information Security Program Components

There are multiple domains and facets to running an information security program. These are documented across multiple information security policy documents which relate to the topics below:

- **Access Control**

  Adequate security of information and information systems is a fundamental responsibility. All applications and networks that deal with financial, privacy, or safety information, must include some form of access and or authorization control. The CalAmp information security team employs a number of tools, technologies, and processes to protect standard and privileged access.

- **Application Security**

  Application security addresses the risk from external threats as application vulnerabilities typically account for the largest number of initial attack vectors after malware infections. With technologies such as a Web Application Firewall, secure coding practices, and continuous assessments, we ensure applications are protected according to standard information security best practices.

- **Asset Management**

  A key component of any program is identifying and documenting assets to remove ambiguity and gaps in asset knowledge. As such, the Company applies a systematic approach to maintaining an asset protection and lifecycle management program that optimizes value.

- **Business Continuity**

  Business continuity is an integral part of securing business operations. The Company employs a comprehensive and documented approach to determine the how, when, where, who, and what will be needed should a disruption of normal operations occur. Business continuity includes managed and well-organized procedures to assure the continuity of operations under extraordinary circumstances, including measures to assure the privacy and security of information resources.

- **Change Management**

  Change management is the process of managing changes, updates, installation, or removal of any hardware, software, interfaces, or databases that impact CalAmp systems. The Company leverages an automated ticketing system to guide the process from beginning to end with consideration for development, testing, quality assurance, and pre-release approvals and post release support services.

- **Data Encryption**

  CalAmp uses encryption tools to protect the confidentiality and integrity of data in transit and data at rest. This applies to data, services, systems, and devices owned, managed, or otherwise controlled by CalAmp, whether on-premises or in the cloud.

- **Incident Management**

  The Incident Management process at CalAmp is a lifecycle approach, which has six phases: Preparation, Identification, Containment, Remediation, Recovery and Follow-up or Lessons learned. This process is utilized to guide internal and external resources (e.g. personnel) including technical specialists which are ready to assist the Company with minimal downtime upon an incident notification.

- **Risk Management**

Engaging in any business-related activity requires appropriate risk management to ensure either maximum return on investment or minimizing potential downside. Risk management covers various aspects of the opportunity costs assessment, risk identification and mitigation, as well as prioritization, control rationalization, and monitoring of control effectiveness.

- **System Security**

All systems and devices on the CalAmp network or controlled by CalAmp whether on-premises or in the cloud, require secure infrastructure that protects the confidentiality, integrity, and availability of customer and corporate data to mitigate security risk. Specific system security requirements are continuously reviewed to ensure that CalAmp has the appropriate safeguards in place.

- **Third Party Risk Management**

Third Party Risk Management enables an organization to utilize external services and resources while ensuring the appropriate quality of technology products and services procured. CalAmp information security performs a robust vetting process to ensure the products and services that are procured align with CalAmp's risk management expectations.

- **Training and Awareness**

CalAmp requires employees to participate in security training, education, and awareness training upon hire and at least annually thereafter. The training and awareness programs include but are not limited to:

- Password policy
- Acceptable use of systems and data
- Access management
- Device management
- Secure connectivity
- Phishing
- Social Engineering
- Physical security
- Incident response
- Data privacy

Additional training can be performed on various security topics, as necessary.

- **Vulnerability and Patch Management**

Technology and supporting infrastructure evolves constantly; therefore, information security needs to adapt to the ever-changing environment. Vulnerability and Patch Management protocols ensure that data and systems are protected while new vulnerabilities are not introduced into the current control environment. Information security utilizes best practices or standards for identifying, classifying, remediating, and mitigating threats and keeping our systems secure.

4.2 Program Procedure Requirements

Information Security Policies – Policies are implemented and enforced to assure the security, reliability, integrity, and availability of CalAmp information assets. The program is broadly described with the following activities:

- Our global risk assessment and evaluation process.
- Establishing and maintaining enterprise-wide security controls for information assets.
- Validating the effectiveness of operating controls through continuous testing and enhancements
- Providing internal and external service provider oversight and 24/7 monitoring.
- Performing periodic reviews and updating of the information security program.
- Reporting key risk as well as operational and program metrics.
- Maintaining appropriate training programs and educational seminars.

There are multiple domains and facets to running an information security program. These are documented across the following documents.

Information Asset Security Procedures – Procedures will be implemented and maintained to ensure compliance with security policies and to assure the security, reliability, integrity, and availability of CalAmp information assets.

Accidental or Unauthorized Events – Policies will be implemented and maintained to protect CalAmp information assets against accidental or unauthorized modification, disclosure, or destruction.

4.3 Exceptions

Exceptions To Policies – All information technology resources connected to CalAmp's networks are expected to comply with CalAmp information security policies and standards which are designed to establish the controls necessary to protect CalAmp's information assets.

A control deficiency in one business process or resource can jeopardize other processes or resources because erroneous data may be inherited, privacy can be compromised or because a conduit for an intrusion into CalAmp's systems may be created. However, there may be a case where compliance cannot be achieved for a variety of reasons.

In such cases, an exception must be documented and approved according to CalAmp's Risk Management processes, and thereafter be reviewed at least annually.

4.4 Policy Distribution

Written Security Policy Documents – CalAmp management will publish and control written information security policies and make them available to all employees and relevant external parties.

Annual Review of Applicable Security Policies – All CalAmp employees and contractors will review and acknowledge acceptance of the information security policies which apply to them at least on an annual basis.

Policy Document Classification – All CalAmp security policy documents will be labeled as "CONFIDENTIAL – FOR INTERNAL USE ONLY" and revealed only to CalAmp workers and select outsiders (including but not limited to auditors) who have a legitimate business need for this information.

4.5 Program Review

Annual Review of Information Security Policy Documents - All CalAmp written information security policy documents are reviewed on an annual basis by members of CalAmp management. Additionally, the Information Security Policy will be reviewed by the Cybersecurity and Data Privacy Committee of the Board of Directors (the "Cyber Committee") on an annual basis.

Quarterly Status Review of Information Security Priorities – The CalAmp information security team will provide quarterly status reviews on critical information security priorities to the Cybersecurity and Data Privacy Committee. If matters are identified during the status reviews that require a change in the written policy documents, the changes will be discussed, and edits will be made for review at the next meeting of the Cyber Committee.

Program Review Input – The CalAmp information security policies will incorporate information and input from the following sources:

- The Cyber Committee.
- Internal audit function for the Company, whether or not outsourced.
- Results of independent reviews of the policy, including but not limited to auditors and customer due diligence reviews.
- Management feedback due to annual reviews, preventive and corrective actions, and compliance assessments.
- Threat and vulnerability trend analyses derived from internal and external resources.
- Reported information security incidents.
- All applicable recommendations provided by relevant authorities.

4.6 Responsibility Assignment

Information Security Department Responsibilities – The Information Security team is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines and procedures. The Sr. Director of Information Security is responsible for facilitating the regular review and approval of these supporting documents with relevant stakeholders.

Information Security Resources – Management will allocate sufficient resources and staff attention to adequately address information systems security.

Management Responsibility – Information Security is a cross-functional responsibility, as such, management works with the information security team to ensure controls are designed, functioning, and adhered to applicable policies, procedures, and regulations.

Clear Assignment of Control Accountability – CalAmp management will clearly assign and document accountability for every internal control at CalAmp. This accountability will provide sufficient transparency so that executive management will be kept informed about the effectiveness and efficiency of these relevant internal controls.

Information Ownership Assignment – The heads of each functional area or department assign information ownership responsibilities for production systems, databases, master files, and other shared collections of information used to support production business activities.

4.7 Program Reporting

Annual Security Program Report - The Information Security team must submit quarterly reports to CalAmp management that include information on:

- The updated risk assessment and analysis.
- The status of the program.
- Management decisions for the level of risk mitigation and residual risk accepted.
- Service provider oversight activities and status.
- The timing and results of testing of key controls.
- Management's response to any identified deficiencies and recommendations for program changes.
- The independent validation of the information contained in the report.
- Updates to the security program from team composition, significant risk changes, or other key programmatic changes while discussed during quarterly cadence, can also occur when necessary, out-of-cycle.

4.8 Security Program Compliance

Laws, Regulations and Contractual Requirements - For every CalAmp production information system, all relevant statutory, regulatory, and contractual requirements must be thoroughly researched, explicitly defined, and included in current system documentation. All third-party required audit activities must be kept to a minimum in order to minimize disruption of daily business operations.

5.0 Additional Considerations for Information Security Program

5.1 Organizational Structure

Staffing requirements – The Information Security team will hire and retain individuals with breadth and depth of experience and knowledge in various facets of Information Security including (but not limited to) data analytics, incident response, identity and access management, programming, internal controls, business process improvement, security architecture, project management, privacy, business continuity and risk management.

Training/Certification – In order to ensure that information security personnel are current with developments within the broader Cybersecurity space, CalAmp will encourage team members to pursue a minimum of one industry certification (Including but not limited to CISSP, CRISC, CISM, CISA, CEH, CEH, CCSP etc.) within 18 months of hire, maintain all relevant certifications, and obtain at least 40 hours of continual professional education per year from an Information Security or Information Assurance Professional Organization/Consortium.

Staff Augmentation/Professional Services – As the information security landscape evolves quickly, there may be instances where it may be more efficient and effective to procure professional services from an external firm than hiring talent or performing internal training, especially for limited term engagements, time intensive activities outside of core security tasks, or one time projects.

CalAmp Information Security department may elect to engage in staff augmentation/professional services to balance internal core capabilities and auxiliary talent/skillset requirements for completing various projects. The Company will perform a robust vendor vetting process to select the appropriate professional services firm. Considerations for an engagement include but are not limited to – expertise in requested field, industries and clients served, length of engagement, involvement of internal personnel, and other factors.

Cybersecurity and Data Privacy Committee – The CalAmp Cybersecurity and Data Privacy Committee consists of key board members with applicable experience in working with technology companies and/or managing cybersecurity and data privacy risks. The Cybersecurity Committee is expected to meet on a quarterly basis to review matters such as the Company's Cybersecurity and Data Privacy strategy, organizational structure and personnel, technology partners as well as key performance indicators (KPI) and risk indicators (KRI), and to discuss and address information security developments (both internally and externally) and prioritize key information security initiatives with relevant stakeholders.

5.2 Program Review Maintenance

Risk Assessments – The information security program will be updated, as appropriate, based on the results of an organization and/or a third-party risk assessment.

Security Assessments – CalAmp shall ensure that annual external assessments are performed by a nationally recognized professional organization to evaluate and ensure the effectiveness of Company information security measures. This includes, but is not limited to, SSAE SOC 2 Type 2 attestation, SOX compliance reviews, NIST Cybersecurity Framework (CSF) reviews, external penetration and attack simulations, or any other regulatory requirement as requested by an external governing entity.

Information System Audit Control Reviews An independent and externally provided review of information systems security must be obtained at least annually to determine both the adequacy of and compliance with controls.

Change Considerations – The appropriate level of expertise must be applied to evaluate whether changes in the organization or infrastructure should trigger a change to the information security program. Changes that should be considered that could require an update to the information security program are as follows:

- Changes in or upgrades to technology.
- The sensitivity of information.
- The nature and extent of threats and the threat environment.
- CalAmp's business arrangements, e.g., mergers, alliances, joint ventures.
- Customer or supplier information systems, e.g., new configurations, new connectivity, new software.

5.3 Cybersecurity Liability Insurance & Incident Response

Cybersecurity Liability Insurance – The risk of data breaches and cyber incidents has increased due to the dynamic and fluctuating nature of the broader technology landscape. Obtaining Cybersecurity Liability insurance is essential in helping CalAmp recover from a data breach / incident and mitigates costs that can include business disruption, revenue loss, equipment damages, legal fees, public relations expenses, technical forensic analysis, regulatory compliance, and legally mandated notifications.

Therefore, CalAmp will maintain Cyber Liability insurance coverage through a syndicate of nationally recognizable underwriters at a level (or amount) which is deemed appropriate by executive management and consistent with other public companies of the same size and complexity as CalAmp.

Incident Response – CalAmp Information Security team will have a core understanding of incident management and response procedures (Data analytics, log review, asset management, technical forensics analysis, preserving chain of custody, documentation) to help facilitate with the research into and remediation of a data breach. A formal written incident response plan has been prepared and documented and will be updated by the Information Security team on an annual basis or more frequently as deemed necessary.

Since data breach containment activity is urgent in nature, CalAmp may elect to have an Incident Response firm on retainer to expedite containment, remediation, documentation, and other incident response activities.