Information Security Guidelines for Suppliers

REVISION DATE: 25 October 2025
REVISION LEVEL: B
OWNER: Director of Cybersecurity

1.0 Introduction

1.1 Kimball Electronics a global, multifaceted manufacturing solutions provider of electronics manufacturing services ("EMS"), including engineering and supply chain support, to customers in the automotive, medical, and industrial end markets. Information and cybersecurity protection is vital to maintaining our operations, and the trust of our business and supply chain partners and our Share Owners. For this reason, Kimball Electronics expects our Suppliers to view information security and cybersecurity as vital and to play a critical role in our information security posture so that we can deliver on the commitments we make to our mutual customers.

1.2 Suppliers who are engaged in providing products or services to Kimball Electronics, Inc. and/or any of its parent, subsidiaries, or affiliates (collectively, "**Kimball**"), who will have access to Kimball data and/or Kimball Systems are expected to abide by the following cybersecurity requirements as applicable to the Supplier's business engagement with Kimball.

2.0 Purpose

These Guidelines establish a minimum baseline of information security and cybersecurity measures that Kimball expects of its Suppliers. Kimball may supplement these requirements in separate Agreements as warranted to account for specific risks associated with Kimball's relationship with a Supplier. The requirements outlined herein serve as a supplement to and do not supersede any information security or cybersecurity-related provisions set forth in such Agreements.

3.0 Scope

These Guidelines' Scope is all new and existing Suppliers to Kimball that (i) access Kimball facilities; or (ii) access, process, store, or transfer Kimball Data; and/or (iii) access or process Kimball Systems that may store, process, or transmit Kimball Data; or are used to access Kimball Systems or Kimball Data.

4.0 Definitions

4.1 **Agreement** means the governing contracts, purchase orders, statements or work (or relevant portions thereof), or other written or oral agreements between the Supplier and Kimball that set forth the scope of and terms products and/or services the Supplier is providing.

4.2 **Confidential Information** means the meaning set forth in any Agreement for confidential information relating to Kimball, howsoever defined. If no such Agreement exists, Confidential Information means any and all non-public, proprietary, or confidential information in any form disclosed by a party (each a "**Discloser**") to the other party (each a "**Recipient**") (i) that has been marked as confidential; (ii) whose confidential nature has been made known by Discloser, orally or in writing, to Recipient; or (iii) that, due to its character and nature, a reasonable person under like circumstances would treat as confidential. Confidential Information also includes all notes, analyses, summaries, and other materials in any form prepared by Recipient or any of its employees, agents, or other representatives ("**Representatives**") that contain, are based on, or otherwise reflect, to any degree, any of the foregoing ("**Notes**"). Notwithstanding the above, Confidential Information shall not include information that Recipient establishes by competent evidence:

a) was generally known or available at the time it was disclosed or has subsequently become generally known or available through no fault of Recipient;
b) was rightfully in Recipient's possession free of any obligation of confidence prior to Discloser's disclosure hereunder;
c) is independently developed by Recipient without access to or use of Discloser's Confidential Information; or
d) was received by Recipient free of any obligation of confidence from an unaffiliated third party, provided that such third party is and was not prohibited from disclosing such Confidential Information by any legal, fiduciary, or contractual obligation.

4.3 **Customer Data** means any information provided to Kimball by its customers in the course of business.

4.4 **Data Protection Laws** mean all applicable laws, regulations, and other requirements of any jurisdiction, self-regulatory organization, or certifying authority relating to privacy, data security, communications secrecy, Security Breach notification, or the processing of Personal Data.

4.5 **Information Security** means ensuring that only authorized users (Confidentiality) have access to accurate and complete information (Integrity) when they require it (Availability).

4.6 **Information and System Security Governance Program** means a program of policies, procedures, standards, defined workflows, and metrics that protect Kimball Data and Systems from unintended or malicious activities, unauthorized access, loss, alteration, misuse, transfer, retention, Threats, and Vulnerabilities. An example of such a Program is Kimball's Information Security Management System.

4.7 **Kimball Data** means Personal Data, Customer Data, Confidential Information, and

any other communications or business records that Supplier receives from Kimball, has access to, or otherwise processes for or on behalf of Kimball.

4.8 **Kimball System** means any hardware, software, media, network or other information technology ("IT") resource, whether physical or virtual, owned, licensed or operated by or on behalf of Kimball, whether on Kimball's premises or connected to or accessible from its network, other than any that are owned by Supplier or its Sub-processors.

4.9 **NIST** means the United States National Institute of Standards and Technology.

4.10 **Personal Data** means any information that relates to an identified or identifiable individual, or that can be used to identify, locate, or contact an individual, alone or in combination with other information.

4.11 **Personnel** means a party's employees, contractors, officers, agents, contingent or temporary workers, and other service providers.

4.12 **Security Breach** means any breach of security leading to the unintended, accidental, malicious, or unlawful access, destruction, loss, alteration, misuse, transfer, or retention of Kimball Data and/or Kimball System(s).

4.13 **Sub-processor** means any service provider, affiliate, or sub-contractor engaged by Supplier for purposes of fulfilling services for or on behalf of Kimball.

4.14 **Supplier Systems** mean Supplier operating systems, applications, hardware, software, media, or devices, whether physical or virtual, that are used to conduct business and facilitate communications with Kimball; that may store, process, or transmit Kimball Data; or are used to access Kimball Systems or Kimball Data, whether on Supplier's (or its Sub-processor's) premises, connected to or accessible from Supplier's (or its Sub-processor) network(s), or hosted in the cloud.

4.15 **Threat** means anything (e.g., object, substance, AI process, human) that is capable of acting against Supplier Systems, Kimball Data, Kimball Systems, Supplier Personnel, or Kimball Personnel in a manner that can result in harm to Kimball Data or Kimball Systems or otherwise cause an unwanted incident involving the same.

4.16 **Vulnerabilities** mean a weakness in the design, implementation, or operation of internal controls in a process that could be exploited to cause a Security Breach or make a Security Breach more likely.

5.0 References

Please refer to the Kimball Electronics Supplier Documentation site (https://www.kimballelectronics.com/documentation/) for the following reference documents that relate to this policy:

5.1 Global Supplier Code of Conduct
5.2 Privacy and Security Notice
5.3 Global Purchase Order Terms and Conditions

6.0 Information Security and Cybersecurity Governance

6.1 The Supplier shall establish and maintain an Information and System Security Governance Program. Such Program may include one certified by an independent authority as complying with the requirements of ISO 27001.

6.2 The Program shall be approved by an appropriate executive; communicated to all relevant internal and external stakeholders, including Personnel; and implemented and reviewed at least on an annual basis and, at a minimum, whenever significant changes in business objectives, processes, Data Protection Laws, or contractual requirements occur.

6.3 The Supplier shall have an effective Information Security organizational structure with significant authority and adequate resources to implement and maintain the Program.

6.4 At a minimum the Program shall ensure that the Supplier:

6.4.1 Maintains appropriate network security measures, including without limitation firewalls to segregate Supplier's internal networks from the Internet, risk-based network segmentation, and intrusion prevention or detection systems to alert the Supplier to suspicious network activity;
6.4.2 Installs and maintains anti-virus and malware protection software with up-to-date definitions and signatures on all Supplier Systems. Such software must be properly configured to protect against Threats, including without limitation viruses, worms, Trojans, rootkits, spyware and keystroke loggers;
6.4.3 Maintains and enforces rules for the acceptable use of data, including Kimball Data, with identified, documented, approved and communicated data processing facilities;
6.4.4 Establishes, documents, and implements, where relevant, commonly accepted industry standards (such MS-SDL, NIST 800-160, and/or Secure-SDLC) to include security requirements within all phases of software development lifecycles;
6.4.5 Identifies and maintains an inventory of assets and facilities associated with data and systems, including Kimball Data, Kimball Systems, and Supplier Systems;
6.4.6 Establishes policies on the use of encryption based on NIST guidelines 800-175B Rev. 1 or equivalent guidelines to protect Information Security;
6.4.7 Develops operating procedures for operational Personnel to ensure correct and secure operations of its facilities where data, including Kimball Data, is processed;

6.4.8 Develops incident handling procedures to ensure a quick, effective, and orderly response to Security Breaches and events impacting Information Security; and

6.4.9 Implements and maintains a business continuity program that includes documented recovery strategies, plans, and procedures, to ensure the continuity of products and services to Kimball within the defined timeframe.

6.5 If the Program is not certified to ISO 27001, the Supplier shall ensure that a third party conducts and documents an independent review of the Program per industry standards on an annual basis or whenever significant changes in business objectives, processes, Data Protection Laws, or contractual requirements occur.

7.0 Supplier Personnel Information Security Requirements

7.1 The Supplier should perform commercially reasonable background verification checks on relevant Personnel that interact with Kimball Data, Kimball Systems, and Supplier Systems. Such checks shall be proportional to business need and performed in accordance with applicable laws, regulations, and the Kimball Electronics Global Supplier Code of Conduct.

7.2 The Supplier shall ensure that all relevant Personnel understand and are suited for their roles and responsibilities related to Information Security and the Program.

7.3 The Supplier shall ensure that all Personnel undergo appropriate training and awareness education under the Program and receive regular updates on Information Security and the Program relevant to their job function.

7.4 The Supplier shall have a formal, written, and communicated disciplinary process to act against Personnel who have violated these Guidelines and/or Kimball's Information Security, based on the nature, intention and gravity of such violation.

8.0 Minimum Access Controls

8.1 The Supplier's Program shall implement appropriate technical safeguards such as encryption in transit or at rest using industry-standard encryption algorithms and secure key management protocols, locked files, cabinets, and other electronic and physical security controls designed to prevent a Security Breach.

8.2 At a minimum, the Supplier's Program shall implement the following access controls for Kimball Data, Kimball Systems, and Supplier Systems:

8.2.1 Appropriately restrict access (consistent with the principles of least privilege, need-to-know, and segregation of duties) to only those Supplier Personnel that require such access to such Data and Systems to perform the Supplier's duties described in the relevant Agreement(s);

8.2.2 Assign unique Supplier-owned/registered access and/or authentication

credentials to each Supplier Personnel with authorized access to such Data and Systems;

8.2.3 Assign unique Supplier-owned/registered business email addresses within a Supplier-owned/registered domain (e.g. employee@Supplier.com) to Supplier Personnel with authorized access to such Data and Systems;

8.2.4 Prohibit sharing of assigned access/authentication credentials;

8.2.5 Protect all stored access/authentication credentials in accordance with security best practices to prevent unauthorized account access;

8.2.6 Implement password security best practices, including without limitation complex password requirements, account lockout controls, periodic password resets, and changing all default passwords before deploying any new hardware or software asset. The Supplier should consider referring to NIST Special Publication 800-5-63 or equivalent guidelines for setting password security best practices;

8.2.7 In cases where remote access is authorized, ensure access to such Data and Systems requires multi-factor authentication (at least 2-factor) and session encryption pursuant to password security best practices;

8.2.8 Promptly disable access privileges to such Data and Systems for any Supplier Personnel who no longer need and/or are authorized such access;

8.2.9 Conduct periodic reviews of access lists to such Data and Systems to ensure that access privileges have been appropriately provisioned and disabled; and

8.2.10 Prohibit access to such Data and Systems from unauthorized devices or via unauthorized tenants in a multi-tenant service (i.e., SaaS, IaaS, PaaS).

9.0 Physical Security, Data Classification, and Data Handling

9.1 The Supplier shall only access and use Kimball Data and Kimball Systems to fulfill its obligations under applicable Agreements or as explicitly directed by Kimball, and for no other purposes.

9.2 Supplier shall comply with all applicable Data Protection Laws in its performance of obligations under Agreements.

9.3 If the Supplier is acting as a data processor under Data Protection Laws, the Supplier must execute a Kimball-approved data processing Agreement.

9.4 The Supplier, when acting as a data processor under Data Protection Laws, should respect and apply the provisions of applicable data processing Agreements and ensure that its Personnel and Sub-processors are made aware of the contractual obligations to protect data, passing on the same contractual obligations to any subcontractors.

9.5 If the Supplier is required by Data Protection Laws or other applicable laws to retain archival copies of Kimball Data, this data backup must be stored in a physically secured facility and in an encrypted format. Encryption keys must not be stored on the system storing the backup. At Kimball's direction, at any time, and in

any event upon termination or expiration of Agreements, except to the extent required by Data Protection Laws or other applicable laws, the Supplier shall immediately (or consistent with another time frame set forth by Kimball) return to Kimball or, if so directed by Kimball, destroy and certify the destruction of any and all Kimball Data consistent with NIST Special Publication 800-88 or equivalent guidelines.

9.6 The Supplier shall ensure that Personnel and Sub-processors immediately return all Kimball Data in their possession upon termination of their relationship with the Supplier.

9.7 The Supplier shall define and use physical security perimeters to protect areas that contain Kimball Data, Kimball Systems, or Supplier Systems. The Supplier shall protect secure areas by appropriate entry/exit control and surveillance measures to ensure Information Security.

10.0 Incident Management

10.1 The Supplier shall develops incident handling procedures to ensure a quick, effective, and orderly response to Security Breaches and events impacting Information Security. Security Breaches and events impacting Information Security must be reported promptly through appropriate management channels.

10.2 The Supplier must report Security Breaches and events involve or impact Kimball Data and Kimball Systems to the Kimball Electronics Support Center. Notification must be made as soon as possible, and in no event more than 24 hours from detection, if Kimball Data, Kimball Systems, or Personal Data are involved.

10.3 Supplier shall cooperate with Kimball in investigating all incidents, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required.

11.0 Kimball's Rights

11.1 Kimball reserves the right in its sole discretion to terminate access to Kimball Data and Systems for any Supplier that (i) fails to implement an adequate Program pursuant to these Guidelines, and/or (ii) where Supplier Personnel are suspected of negligence or misuse of Kimball Data or Systems. Kimball's decision to terminate access to Kimball Data or Systems does not waive any of Kimball's claims against Supplier or waive or release Supplier from any of its obligations of performance under these Guidelines and any applicable Agreement, and does not give rise to any claims from Supplier or Supplier Personnel against Kimball.

11.2 Without limiting any other audit rights of Kimball, Kimball shall have the right to review the Supplier's Program prior to the commencement of any Agreement and from time to time during the term of the Agreement. During the term of any Agreement, on an ongoing basis from time to time and with advance notice, where

reasonable, Kimball, at its own expense, shall be entitled to perform or to have performed an on-site audit of the Supplier's Program. In lieu of an on-site audit, upon request by Kimball, the Supplier agrees to complete, within thirty (30) calendar days of receipt, an audit questionnaire provided by Kimball regarding the Supplier's Program. The Supplier shall implement any required safeguards as identified by Kimball or by any audit of the Supplier's Program.