

	<h1>Counterfeit Control Plan</h1>	
Doc Number: POL-134	Home Manual: Business Management System	Page 1 of 5
Version: 4.0		

1.0 Purpose

This policy defines DigiKey's plan to prevent the purchase, acceptance, and distribution of Counterfeit Product (as defined below) within DigiKey's operations.

2.0 Scope

This Counterfeit Control Plan and its procedures apply throughout DigiKey's operational life cycle, including, but not limited to, purchasing, receipt, identification, storage, and distribution. DigiKey has communicated the Counterfeit Control Plan throughout its entire organization and works to ensure that it is understood, implemented, and maintained at every level. The Counterfeit Control Plan applies to all persons doing work under DigiKey's control and to every purchase and sale of Products (as defined below).

3.0 Definitions

3.1 "Product" means electronic components, assemblies, supplies, and equipment.

3.2 "Counterfeit Product" means a fraudulent Product being represented, identified, or marked as genuine but that is actually an unlawful copy, imitation, or substitute of a Product, and any Product that is illegitimately altered by a party other than the manufacturer or a manufacturer-approved source with the intent to mislead, deceive, or defraud the recipient of such Product.

4.0 Procedure

4.1 Commitment to the Counterfeit Control Plan

1. DigiKey and its management are committed to preventing the purchase, acceptance, and distribution of Counterfeit Products. As evidence of this commitment, the Counterfeit Control Plan, including, without limitation, each of the key components identified herein, has been adopted and approved directly by DigiKey's senior management.
2. DigiKey is also a member of the following groups in an effort to educate customers and further decrease the number of Counterfeit Products in the market:
 - A. The Electronic Components Industry Association ("ECIA") in North America,
 - B. The Electronic Component Supply Network ("ECSN") in the United Kingdom, and
 - C. The China Electronics Distributor Alliance ("CEDA") in China.
3. By developing, implementing, and adhering to the Counterfeit Control Plan, DigiKey is certified to the AS6496 standard for mitigating and preventing the proliferation of fraudulent/counterfeit electronic parts through the Performance Review Institute's Counterfeit Avoidance Accreditation Program ("CAAP"). In addition, DigiKey is also certified to the ISO 9001:2015 and ANSI/ESD-S20.20-2021 standards.

4.2 Counterfeit Mitigation Procedure

1. Purchase of Product

- A. To decrease the risk of Counterfeit Products entering into DigiKey's supply chain, DigiKey purchases Products primarily from the manufacturer directly or from manufacturer-approved sources, thereby resulting in DigiKey obtaining Products that are new, authentic, and fully warrantable by the direct manufacturer and for which accurate up-to-date technical information is readily available. DigiKey does not purchase refurbished Products for re-sale.

- B. Authorized manufacturers and manufacturer-approved sources are continually assessed via review of Government Industry Data Exchange Program (“**GIDEP**”) product alerts and supplier quality data.
- C. If DigiKey agrees to distribute Products that are not obtained directly from the manufacturer or a manufacturer-approved source, DigiKey will notify its customers in writing at the time of their respective quotation about the unauthorized Product for which they are being quoted. Moreover, DigiKey will notify its customers in writing of any termination of a manufacturer’s or manufacturer-approved source’s authorization with respect to a Product after the respective customer’s quotation for the Product and prior to DigiKey’s performance thereunder.

2. Traceability of Product

- A. DigiKey retains records that provide the supply chain history of its Products including documentation of all supply chain intermediaries and significant handling transactions.
Note: The purpose of these records is to allow DigiKey to be able to trace its Products backwards from DigiKey to the manufacturer or any manufacturer-authorized source.
- B. Where possible, DigiKey obtains a certificate of conformance for such Products and includes such certificates in its traceability records.

4.3 Customer Related Processes

1. Provision of Manufacturers’ Warranties

- A. DigiKey transfers to its customers, at the time of sale, to the extent transferrable, the warranties DigiKey receives from manufacturers with respect to the Product sold by DigiKey. Copies of manufacturer warranties are available prior to the purchase of Products by contacting DigiKey.
- B. Returns relating to manufacturers’ warranties are subject to the terms and conditions of the applicable manufacturer’s warranty and the applicable manufacturer’s return policies for the Product, provided certain Products are not eligible for return as specified in [Section 4.3\(3\)](#) below.

Example: Some Products may require return directly to the manufacturer or a manufacturer-approved source.

2. Provision of Distribution Agreements

- A. DigiKey retains distribution agreements with the manufacturers for which DigiKey distributes.
Caution: Distribution agreements are considered proprietary and not subject to review by third parties unless mutually agreed upon by both DigiKey and the manufacturer.
- B. DigiKey retains a letter from the manufacturer or is listed on the manufacturer website as evidence of DigiKey’s authorized distributorship.

3. Customer Returns

- A. DigiKey follows a strict returns policy that is outlined in DigiKey’s [Terms of Use and Conditions of Order](#) available on DigiKey’s website. A Product is not eligible for return, refund, or exchange if it is:
 - 1. Purchased from a third party rather than DigiKey directly;
 - 2. A Counterfeit Product;
 - 3. Specifically designated as “Non-Cancellable/Non-Returnable” (“**NCNR**”) at the time of quote or sale; or

4. An electronic-discharge sensitive Product that has not been handled according to the most recent version of the ANSI/ESD-S20.20 Standard published by the American National Standards Institute (ANSI) and EOS/ESD Association, Inc.

B. DigiKey's returns policy includes, among other things:

1. Confirmation of traceability of the Product from DigiKey to the customer, including manufacturer date and lot codes, original purchase date, part number, and quantity.
2. Incoming inspection by designated personnel to assure that all parts are undamaged, in the original packaging, and authentic. Broken or damaged manufacturer's packs are reconfirmed as authentic by DigiKey's designated personnel in conjunction with the original manufacturer.
3. Testing for static damage where appropriate.
4. Testing moisture levels with re-baking where necessary.

4.4 Control of Suspect, Fraudulent, and Confirmed Counterfeit Parts

1. Suspect Parts

If DigiKey suspects, in its sole discretion, that any Product is a Counterfeit Product, DigiKey will quarantine such Product for further testing until such time as a determination about the genuineness of the Product can be made and will take such other actions as may be required or permitted under applicable law and AS6496, including, without limitation, the actions set forth herein.

2. Reporting Confirmed Counterfeit Products

- A.** If a Product is determined to be a Counterfeit Product, DigiKey will report its findings, as appropriate, to:
1. Affected customers;
 2. Applicable DigiKey employees;
 3. The governmental organization at the federal, national, state, or local level having jurisdiction over the Counterfeit Product;
 4. GIDEP; and
 5. Any applicable governmental or regulatory reporting agency or organization.

3. Quarantining and Scrapping Counterfeit Products

- A.** If a Product is determined to be a Counterfeit Product, DigiKey will quarantine the Counterfeit Product for a period of five (5) years, or longer if required by applicable law.
- B.** After the applicable quarantine period, the Counterfeit Product will be irreversibly altered so as to render the Counterfeit Product, including the internal elements, physically and completely unusable.

Caution: Under no circumstances will a Counterfeit Product be restocked or returned to a customer, manufacturer, or manufacturer-approved source as part of a stock rotation.

4. Inventory Control Plan

- A.** Inventory access is maintained with ID card access. Visitors are escorted at all times.
- B.** All Products from unauthorized sources, including any that are returned or restocked, are segregated from Products coming directly from a manufacturer or manufacturer-authorized source pursuant to DigiKey's internal Physical Security Policy.

- C. When possible, DigiKey sends Products in their original manufacturer packaging. If this is not possible, DigiKey uses best commercial packaging practices while observing product electrostatic and moisture sensitivity requirements. Additional packaging procedures and controls are set forth in DigiKey's [Basic Packaging Instructions](#).

4.5 Training

All persons doing work under DigiKey's control are given "Counterfeit Part Avoidance" e-learning training about counterfeit prevention awareness. Also, specialized training is provided to applicable departments and appropriate individual positions to enhance employee competencies in detecting Counterfeit Products, such as the "My role in Counterfeit Part Avoidance" e-learning training.

4.6 Traceability, Record Retention, and Retrievability

1. Register of Manufacturers and Manufacturer-Approved Sources

DigiKey maintains a register of its manufacturers and manufacturer-approved sources within its purchasing software that includes authorization status, approval status, and the scope of approval.

2. Military Parts

It is DigiKey's intent to only sell Commercial Off-the-Shelf ("COTS") parts. If this changes, required documentation and procedures will be updated accordingly.

3. Commercial and Industrial Parts

All Product purchased from DigiKey has a "Certificate of Conformance" printed on the pack list. This information is stored in DigiKey's secure record retention software in accordance with its [Record Retention Policy](#).

4. Retention Period

DigiKey maintains purchase order information in its secure record retention software for the applicable period of time set forth its [Record Retention Policy](#).

5. Certificate of Conformance

- A. DigiKey's Certificate of Conformance that is printed on every pack list contains the following information:

1. Name and address of DigiKey and the customer;
2. Manufacturer's name;
3. Manufacturer's part number;
4. Quantity shipped;
5. Date Code (when available);
6. Lot Code (when available);
7. Customer's Purchase Order Number; and
8. Ship Date.

6. Scrap Control in Authorized Distribution

- A. DigiKey outsources its destruction of all Counterfeit Products, requires a certificate of destruction from third-party providers for all Products scrapped, and maintains a record of all certificates of destruction that it receives.
- B. DigiKey maintains a similar record regarding the disposition of all Products that it suspects of being Counterfeit Products but that are ultimately determined to be genuine.

		Counterfeit Control Plan	
Doc Number: POL-134		Home Manual: Business Management System	Page 5 of 5
Version: 4.0			

4.7 Audits

Counterfeit avoidance is part of DigiKey’s scheduled internal audit program and DigiKey is subject to third-party audits as required.