Security Authentication Verification Policy Sample

Version: 1.0
Date: October 12, 2021

Policy summary: as [company name here] confidentiality and security framework is based on ISO/IEC 27001, this policy introduces a verification process for during the first point of contact with a user. The purpose of this policy is to action steps which are actioned by developers to make administrative changes to a codebase from users who are not an authorised owner, administrator, or reach out with an anonymous/personal email address which is not associated with the codebase. This policy extends to all employees or personnel who access encrypted codebase systems or backend CRMs that manage deployments.

The following scenarios may fall under this criteria for any requests, updates or access to the information below. Please refer to the Appendix for more information related to each criteria:

A. Owner or main administrator email address
B. Financial data and payments
C. Permissions, privileges, and account or administrative rules
D. Standard or general account data
E. Confidential and sensitive information

Policy for verifying codebase information:

Step 1. First step is to verify the validity and authentication for any email address requesting access to the codebase.

Step 2. If the client reaching out has an email address which matches an administrator, or user on record, we can proceed to follow the request as normal. If the email or reference does not match, ask for the following information:

1. Verify the last four digits of a credit card
2. Ask for the most recent invoice or purchase order number
3. If 1-2 cannot be verified, please identify the following information:

A. Request contact information for a member of the Human Resource Department
B. Review company registration or validity of the contact

Please note: do not disclose any information, data, or make changes to the user under review who is requesting access to a codebase. If you find any activity suspicious, spam-related or are unable to verify information to please alert the security division as soon as possible.

Appendix

A. Administrative email address or owner: including, but not limited to account owner name(s) or aliases, email addresses, organisation data, and any information relating to the codebase or related administrator(s).

B. Financial data: including, but not limited to any payment information or terms, payments, invoice history, credit card data, banking, wire transfers, purchase order data, billing addresses, and personal information.

C. Permissions, privileges, and account or administrative rules: including, but not limited to requests or alterations of any type of user access, amendments to access rights, or revoking to access rights.

D. Standard or general account data: including, but not limited to content management, applications, integrations, API keys, developer tools, and tracking information.

E. Confidential information: including, but not limited to any sensitive, personal or private data related to the account. According to the Privacy Act of 1974, enacted by The United States Department of Justice, as amended, 5 U.S.C. § 552a, establishes a code of fair information practises that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.