Secure Code Warrior Security Policy

Public Version 1.0
Author: Secure Code Warrior Trust Team
Date: April 2021

Introduction

Secure Code Warrior recognizes that information and the systems that process information are valuable assets which are essential to Secure Code Warrior. Secure Code Warrior management recognizes the importance of protecting information from internal and external threats and recognizes that effective information security management is critical in order to ensure the continuation of Secure Code Warrior services to our customers and business functions for our employees and contractors. Secure Code Warrior management is committed to preserving the confidentiality, integrity and availability of all physical and electronic assets.

In case you want to raise a security incident, please send an email to security@securecodewarrior.com

Scope

Development and operations of SaaS platform for improving "secure software development" competences.

Organization of Information Security

Management has the overall responsibility for managing Secure Code Warriors values in an effective and satisfactory manner according to current laws, requirements and contracts.

The Security Board, chaired by the CTO, has the overall responsibility for information security at Secure Code Warrior, including information security regarding personnel and IT security.

Human Resources Security

- Secure Code Warrior shall ensure that all people requiring access to sensitive information assets at a privileged level either as employees or by third-parties are subject to background checks in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
- Employees and third-party users shall agree and sign the terms and conditions of their employment contract with their own employer, which shall state their employer's organization responsibilities for information security.
- Management shall be responsible for ensuring that employees and third-party users apply information security in accordance with the established policies and

procedures of Secure Code Warrior;
- All employees and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their activities for Secure Code Warrior;
- All employees and third-party users shall be made aware that causing a breach of information security or non-adherence to information security policy requirements may result in disciplinary action;
- Secure Code Warrior shall implement a process to ensure that terminations, resignations and changes of job responsibilities maintain an adequate level of information security;
- Secure Code Warrior shall implement a process to ensure that all employees and third-party users shall return all Secure Code Warrior data, equipment and access means in their possession upon termination of their employment contract or agreement;

Asset Management

Classification of information

Secure Code Warrior has defined the following information classification scheme:

- **Public**: all information publicly available, generally well known or free of confidential content are public. All other categories of information are therefore non-public. Disclosure of public information causes no harm to Secure Code Warrior. E.g. company website, Gartner reports, ...
- **Internal**: all information that is to be used only in a company internal context. This information is not to be made public without prior authorization from management. Disclosure of internal information could cause minor embarrassment or operational inconvenience. E.g.: internal email list or phone numbers
- **Confidential**: confidential information is all information concerning the internal workings and processes of Secure Code Warrior. Disclosure of confidential information can have serious short term or long term impact on operation and strategic objectives. E.g.: financial data, customer data or administrator passwords, etc.

Secure Code Warrior handles assets according to its classification by implementing access restrictions and protecting information to a level consistent with the information classification.

Media handling

- Secure Code Warrior does not allow any data (other than public data) to be copied on disposable media.
- Physical copies of data are discouraged

Access Control

- Users must be uniquely identified through a personal User Identifier (ID) on each system & application they received access to;
- The user ID assigned to a user shall unambiguously be tied to him/her;
- Access to system components must be restricted to those individuals whose job requires such access;
- Access requests recorded and managed via a centralized system.

- Group, shared and generic accounts and passwords must be prevented or clearly justified.
- User ID of the individual terminated must be immediately deactivated (Not removed) on every system he or she had access to. Deactivation must be initiated by HR. Inventory of access rights (Individual, role, system resources, User ID, status) must always reflect the exact situation;
- Revoked User ID's shall not be reassigned to other individuals.
- Accounts not used for more than 180 days must be disabled or justified;

Physical Security

Secure Code Warrior operates in a cloud native environment, however (where applicable) the following measures will be undertaken;

- Office premises must be equipped by electronic badge access control
- Individual access badges may not be shared.
- All visitors should be accompanied during their visits. It is the responsibility of the visited Secure Code Warrior staff to accept a 'non-staff' person into the office.
- Computers (desktops and laptops) shall be left locked when unattended;
- Employees, consultants must not leave unattended sensitive (restricted, or private) information on their desk and printers.

Operations security

- Changes to the production platform are controlled and where relevant for information security are approved prior to implementing.
- The use of production resources is monitored and logs are kept, capacity management ensures that the proper resources are available when needed.
- Development, test and production environments are separated to reduce risk.
- Underlying operating systems that only contain necessary components and configuration.
- Secure Code Warrior takes regular backups of information such as customer data, configuration files, instances etc.
- Backups are periodically tested.
- Secure Code Warrior maintains event logs which serve as an audit trail for actions performed and include specific alerts to be sent to administrators when irregular activity occurs.
- Log information is protected against unauthorized access or tampering.
- Logs are retained for at least 30 days.

Cryptography

- All software assets used to store data shall only be available over a secure (TLS/SSL/HTTPS) channel.
- Secure Code Warrior devices containing confidential data will be encrypted.

Supplier Relationships

- Agreements with suppliers that handle Secure Code Warrior information address security requirements to ensure the supplier meets Secure Code Warrior security standards, this includes:
    - requirements regarding subcontracting.
    - a description detailing the purposes for which the supplier has access to Secure Code Warrior information.
    - security measures to be taken by the supplier.
- Secure Code Warrior monitors, and where necessary audits, supplier service delivery including security requirements.

System Acquisition Development and Maintenance

Security requirements of information systems

- New information processing systems or software are subject to specified security requirements to be decided upon before using or activating new systems or software.
- Information travelling on public networks is secured and cannot be intercepted in plain text.

Security in development

- Secure Code Warrior has established guidelines for secure development.
- Secure Code Warrior regularly performs security testing of its platform (both external tests and automated built in tests), any issues or bugs are registered, planned and fixed.
- External pentests are planned and executed regularly.
- Critical security vulnerabilities will be fixed or patched with the highest priority.

Test data

- Test data is carefully selected, protected and controlled. Production data can only be used for testing after proper anonymization of the data.

Information Security Incident Management

- Security incidents are reported as soon as possible using our incident management process, including information that can be used to collect evidence. Raising a potential security incident can be done via email to security@securecodewarrior.com
- Employees and contractors are aware of their obligation to report any (suspected) security incidents or events.
- When an incident has been resolved, those responsible will evaluate the incident to determine any required corrective actions to be taken to reduce the likelihood or impact of future incidents.