Review date: 9/4/2024

SISTERNA®

SECURITY

INTRODUCTION

Providing security for the knowledge and documents present at Sisterna is an important topic, which important is increasing over the years. We do not only want to keep our information secure but we also want to protect the privacy of our employees and our partners.

Several precautions have been taken to ensure the security. These precautions are mentioned in this document. We try to keep up-to-date with the newest development in this area.

We hope that by taking these measures we reduce the chance and impact of a possible security risk.

Sincerely,

Miranda Huppertz & Christel Wouters
Managing Directors Sisterna BV

SAFETY OF EMPLOYEES

We guarantee a safe and healthy working environment for every employee. We do this by following a plan to ensure that the risk in the working environment is as low as possible and we take several measures to uphold this working environment. One of them being that we conduct a risk assessment and evaluation (RI&E).

SYSTEM SECURITY

Our system administration is managed by VSA (www.vsa.nl). They ensure our system is backed up using Acronis Backup Advanced for Hyper-V (v 12.5) with shadow copy backups performed twice daily at fixed times on working days. All systems are equipped with AV-Defender and Datto EDR, which are monitored via the Datto EDR & Security Dashboard. Additionally, laptops are secured with BitLocker encryption and password-protected booting.

Rocket Syber provides 24x7 monitoring to detect unauthorized actions. In the event of a security incident, Rocket Syber (based in the U.S.) notifies Security or the first-line standby employee. Our firewall (Stormshield) offers real-time protection, control, monitoring, and SD-WAN connectivity.

Sisterna also has an APC Smart-UPS emergency power supply with PowerChute software. To enhance security, all Sisterna employees regularly change their passwords. Employees also use webcam covers on their laptops to ensure privacy, even in the event of a security breach. An ad blocker is installed on all systems to block unsafe advertisements and pop-ups.

Employees who work remotely connect via a Remote Desktop Gateway secured with a certificate. This connection is further protected by two-factor authentication (2FA) through the ESET Secure Authentication App on their smartphones.

CONFIDENTIALITY

The nature of each employees work entails obtaining knowledge of confidential communications and/or confidential information from employer, affiliates, sister companies, suppliers and clients. All activities are of a strictly confidential nature. The employee is obliged to observe strict confidentiality during and after the end of the assignment or work.

The employer is bound to confidentiality with regard to all that has become known to him about the personal circumstances of the employee of which he can reasonably suspect the confidential nature. This duty of confidentiality continues to exist even after termination of employment.

Violation of the duty of confidentiality leads to the dismissal of the employee. A penalty clause is included in the employment contract. The duty of confidentiality during and after termination of employment is included in the employment contract.

This is also stated in the working conditions of Sisterna.

WHISTLE BLOWER PROCEDURE

If an employee of Sisterna wants to report on wrongdoing, incident, suspicion or anything else of this matter a confidential advisor is appointed within Sisterna to which these matters can be reported. The confidential advisor reports to the management if suspicious action is found or reported from other employees. This is also stated in the working conditions of Sisterna.