CODE OF CONDUCT

CC–009E v 2.0

CONTRACTOR SECURITY CODE OF CONDUCT

COVER

Title	Contractor Security Code of Conduct
Classification	Code of Conduct
Document code	CC-009E
Approved by	Nexi Group CISO
Approval date	08-05-2024
Date of entry into force	08-05-2024

UPDATES

Version	Date	Code	Updates
1.0	07-07-2023	CC-009E v 1.0	First issue.
2.0	08-05-2024	CC-009E v 2.0	Annual review. Added security behaviors for the use of generative AI.

TABLE OF CONTENTS

1 INTRODUCTION 4
1.1 APPLICABILITY 4
1.2 ENFORCEMENT 4
2 CONTRACTOR SECURITY CODE OF CONDUCT 4
2.1 INFORMATION PROTECTION 4
2.2 PHYSICAL SECURITY 5
2.3 CLEAN DESK AND CLEAR SCREEN 5
2.4 SECURITY OUTSIDE NEXI PREMISES 5
2.5 SECURITY IN MEETINGS 5
2.6 ACCESS TO INFORMATION, IT EQUIPMENT AND IT SERVICES 6
2.7 ACCEPTABLE USE OF IT EQUIPMENT AND IT SERVICES 6
2.8 ACCEPTABLE USE OF E-MAIL, INTERNET AND SOCIAL MEDIA 7
2.9 ACCEPTABLE USE OF GENERATIVE AI 7
2.10 SECURITY INCIDENT REPORTING AND HANDLING 7
3 SECURITY MONITORING OF USER COMMUNICATIONS AND IT EQUIPMENT 8
4 GLOSSARY 9

1 INTRODUCTION

Nexi Group (“Nexi”) provides contractors with access to information and technologies to enable them to fulfil their contractual obligations. These may include, but are not limited to, information assets owned or governed by Nexi (“corporate information”), workstations (desktops, laptops and thin clients), mobile devices (e.g. smartphones, tablets), storage media (e.g. hardcopy documents and removable storage devices), network services (e.g. internet and e-mail) and software.

Nexi has established this Security Code of Conduct to set the principles and rules for the acceptable use of corporate information and technology resources.

1.1 APPLICABILITY

This Security Code of Conduct applies to contractors of Nexi Group companies and functions who have access to Nexi’s non-public information assets or premises. Contractors are responsible for the continuous alignment of their activities related to their contractual obligations with this Security Code of Conduct.

1.2 ENFORCEMENT

Failure to comply with Nexi Group Contractor Security Code of Conduct may lead to sanctions as defined in the contract. Deviations from this Security Code of Conduct must be formally approved by Nexi and managed appropriately.

2 CONTRACTOR SECURITY CODE OF CONDUCT

As a contractor of Nexi, you are obliged to protect and handle corporate information in any form (physical, electronic and verbal) responsibly and in compliance with the rules and principles set out in this document, which are based on the Nexi Group Security Policy.

You are expected to act ethically, responsibly, professionally and in accordance with local laws in your work related to Nexi and when representing Nexi.

If you are granted access to Nexi premises, corporate information or IT services, you must be familiar with Nexi’s security regulations and comply with the regulations related to your contractual obligations. Your Nexi line manager is responsible for identifying the relevant security regulations.

You are not allowed to circumvent Nexi's security measures. This applies to the physical security measures of Nexi 's premises as well as the protection mechanisms and configuration of IT equipment, IT services and software.

You must attend all security awareness and training activities as required by Nexi.

2.1 INFORMATION PROTECTION

You must handle corporate information with discretion and care in accordance with the Nexi Group Information Classification (Public, Internal, Confidential, Strictly Confidential) and Nexi information handling practices throughout their entire lifecycle as instructed by your Nexi line manager.

You must share and store information only on Nexi-approved platforms, channels and communication methods such as e-mail, SharePoint, Teams, OneDrive and other business collaboration tools, shared folders, verbal, hard copies. Make sure that:

- There is a valid Nexi business reason for sharing the information
- All intended recipients and individuals gaining access to the information are authorized to access it
- Non-Nexi employee recipients have signed a non-disclosure or confidentiality agreement.

You are not allowed to use your personal accounts on Internet services (e.g. e-mail, cloud file storage and sharing platforms, social media and forums) for fulfilling your contractual obligations with Nexi. The use of accounts issued by your company must be explicitly authorized by Nexi.

2.2 PHYSICAL SECURITY

Keep your Nexi-issued ID, access or guest card visible while on Nexi premises. Do not wear it visibly outside Nexi premises.

Keep your ID, access or visitor cards safe and never leave them unattended.

Do not share or lend your keys or ID, access or guest cards to anyone or let others, even colleagues, into Nexi premises without a Nexi-issued ID card or valid guest card and valid access rights.

2.3 CLEAN DESK AND CLEAR SCREEN

Follow the Clean Desk and Clear Screen Policies, as defined here, to protect corporate information:

- If you have confidential material to store on site, inform your Nexi line manager and ask them to provide you with a secure storage place
- Do not leave confidential material unattended on your desk or work area. Store documents in a locked cabinet, drawer, fireproof safe, designated secure room or the like when they are not actively used to prevent unauthorized access
- Securely dispose of redundant hard copies
- Remove documents (original, printed and copies) immediately from photocopiers, printers, fax machines and scanners
- Lock your workstation and other devices with a password-protected screen saver when you leave them
- Do not leave your work equipment or personal items exposed in shared workspaces at the end of the working day
- Turn off your workstation at the end of the working day.

2.4 SECURITY OUTSIDE NEXI PREMISES

Protect corporate information and IT equipment containing or accessing corporate information against physical security threats, such as theft, loss, damage or unauthorized access outside Nexi premises:

- Follow the Clean Desk and Clear Screen Policies also outside Nexi premises
- When you travel, keep IT equipment and work documents in your possession as hand luggage. Do not leave them unattended in e.g. parked vehicles
- Make sure that conversations, phone calls and virtual meetings cannot be overheard
- Make sure that the information on the screen of IT equipment is not visible to unauthorized parties, e.g. with a privacy filter
- Show general vigilance to your surroundings.

To the extent possible, make sure that your remote workspace is as secure as your workspace in Nexi premises.

Connect to Nexi's network infrastructure via Nexi-approved remote access methods and follow Nexi rules for secure connection to the work environment.

2.5 SECURITY IN MEETINGS

Follow secure meeting practices in **meeting rooms**:

- Close the doors and blinds to limit the visibility to the projected information to the people within to room
- Use only approved equipment (e.g. projectors) and (wireless) network for presentations

- Clean the whiteboards and remove used papers from flipcharts and other documents from the room after the meeting.

Follow secure meeting practices in **virtual meetings**:

- Make sure that the confidentiality of the information shared in virtual meetings is maintained, especially when you enable video recording or screen sharing. Under no circumstances allow remote control to your workstation
- Grant access only to those participants waiting in the video conference lobby whom you have invited to the meeting.

2.6 ACCESS TO INFORMATION, IT EQUIPMENT AND IT SERVICES

Access and use only those corporate information and technology resources and services you are authorized to access and use. Do not attempt to access or use information, software, systems, networks or other corporate resources you do not need for your assigned work.

Use only Nexi-approved methods for authentication (e.g. PIN code, username/password, biometrics) as instructed by your Nexi line manager.

As you are solely and fully responsible for all actions taken using your Nexi user accounts, you must safeguard your Nexi user accounts and authentication credentials (e.g. passwords, pins, tokens):

- Do not use other users' accounts and do not allow others to use your accounts
- Keep your authentication credentials strictly secret and do not share them
- Never write them down on paper, in unprotected electronic files or save them on web browsers or applications (autocomplete). Use Nexi-approved password management software to store the authentication information.

Do not use your Nexi e-mail address, user IDs or authentication credentials for non-Nexi governed services or personal purposes.

You must comply with the Nexi password policy and create strong passwords.

2.7 ACCEPTABLE USE OF IT EQUIPMENT AND IT SERVICES

Use only Nexi-approved IT equipment and IT services, including electronic communication and information transfer methods, to access corporate information and technology resources and use them in a responsible, professional, ethical and lawful manner as instructed by your Nexi line manager.

Access corporate information and Nexi technology resources only with approved access methods, such as VDI or jump host.

Mobile devices that access corporate information or technology resources must be controlled through Nexi Mobile Device Management solution.

You may only use software and applications approved by Nexi to fulfill your contractual obligations. If Nexi has provided you with IT equipment, you may only install and download software and applications approved by Nexi on the IT equipment and even then, only if you are authorized to do so.

IT services and IT equipment provided by Nexi are Nexi's property, as well as the corporate information stored on them. Handle them with care, protect them, use them only for the authorized purposes and do not lend them to or share them with others (including family members).

Copy, transfer and store classified corporate information on Nexi-approved removable media only if you are explicitly authorized by your Nexi line manager.

You must not use Nexi's IT equipment or IT services for personal purposes.

2.8 ACCEPTABLE USE OF E-MAIL, INTERNET AND SOCIAL MEDIA

Use your Nexi-issued e-mail address for sending and receiving corporate information. If you have not been issued one, use the e-mail address provided by your company.

Do not send non-public corporate information to other Third Parties without verifying that they are authorized to access the information.

Never send confidential or strictly confidential corporate information by e-mail or over the Internet without authorization and appropriate protection with security controls, such as encryption or password protection. Note that encryption keys and passwords must be exchanged with the authorized recipients using *another* approved and secure communication channel (e.g. phone, SMS, corporate messaging platform).

Do not forward Nexi e-mail messages or corporate information to your or someone else's personal e-mail accounts.

Do not publish corporate information or anything that relates to Nexi's work environment on the Internet, social media or other internet services unless you are authorized to do so, and the information is clearly classified as public.

2.9 ACCEPTABLE USE OF GENERATIVE AI

Generative AI tools may be used at work adhering to the following rules:

- Use of information assets owned or governed by the Group ("corporate information") is allowed only through Nexi Group approved Generative AI tools
- Other Generative AI tools are only allowed to use without any information assets owned or governed by the Group ("corporate information")
- Content produced with Generative AI tools inherit the same level of classification as the input information provided to it. Hence, user must handle the Generative AI content according to its level of classification, ensuring alignment with the required security standards
- Never use Generative AI tools to target any individual or group with threats, intimidation, insults, degrading or demeaning language or images, promotion of physical harm
- User must be very careful to not use Generative AI tools to support unlawful activities like active attacks or malware campaigns that cause technical harms, such as delivering malicious executables, organizing denial of service attacks, or managing command and control servers
- Always make sure that results from Generative AI tools you intend to rely on, or use, are accurate, not misleading or biased, do not violate any other individual or entity's intellectual property or privacy, and comply with Nexi Group's policies, principles and applicable laws.

Please see other internal regulation for further behaviors related to Generative AI tools usage.

2.10 SECURITY INCIDENT REPORTING AND HANDLING

Be vigilant to detect any suspicious or unusual events that may indicate or escalate into a security incident, such as unexpected messages on the screen, reboots, overload of system assets and delays.

Report suspected security incidents to your Nexi line manager and the Nexi Cyber Security Defense Center as soon as possible. Follow the applicable local procedures and established communication channels.

During security incident handling:

- Do not attempt to hide, investigate or resolve the event on your own
- Fully cooperate with the authorized security incident response team during the investigation

- Provide all relevant information with completeness and accuracy and in no case hide or alter evidence
- Do not compromise emergency response under any circumstances.

3 SECURITY MONITORING OF USER COMMUNICATIONS AND IT EQUIPMENT

When you are using corporate information, IT equipment and electronic communications may be monitored and are not private. Monitoring will be carried out in compliance with the local laws and regulations and with privacy protection legislation following the principles of 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimization' and proportionality.

In this context, the appointed staff may access user's information processed via Nexi e-mail account or stored on Nexi IT equipment exclusively for the protection of Nexi corporate information and interests. IT equipment that is suspected to contain known security vulnerabilities, is associated with malicious, illegal or harmful activities or violates the Nexi Group Security Policy may be disconnected from Nexi's network.

4 GLOSSARY

Term	Definition
Approved/authorized	Approved/authorized by Nexi Group or Nexi Group company/subsidiary
Corporate information	Information assets owned or governed by Nexi Group, including Nexi Group's customer information.
Information lifecycle	Creation, use, processing, storage, copying, transmission, disposal
IT equipment	Equipment that supports information processing activities, such as workstations, mobile devices, servers, monitors, keyboards, printers, drives, telecommunications equipment and digital storage media.
Mobile device	A handheld device that provides computational and communication capabilities, such as smartphones and tablets.
Personal account	Account created for personal use and not issued by Nexi Group or contractor's employer for professional, work-related purposes.
Personal equipment	Equipment owned by the contractor for personal use and not issued by Nexi Group or contractor's employer for professional, work-related purposes.
Workstation	A computer intended primarily for professional purposes, which is commonly connected to a local area network and runs end-user applications. Workstations include desktops, laptops and thin clients.