Acceptable Usage Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

CNTXT is committed to safeguarding the data processed by its staff, software, or services. Our customers, partners, and other stakeholders depend on us to take appropriate measures to protect the data in our possession. Thus, each staff member needs to understand how to responsibly use our systems so that we appropriately safeguard the data in our possession.

2. Scope

This policy applies to all staff members, including employees, contractors, consultants, temporary, and other workers that interact with CNTXT systems. All such individuals are responsible for exercising good judgment in appropriately using electronic devices, data, and network resources in accordance with policies and standards, local laws, and regulations. This policy applies to:

- Any company-issued electronic, computing, storage, or network device.
- Any company-owned systems on the Internet or Intranet accessed wirelessly, including but not limited to servers, software, operating systems, storage, and network accounts.
- Any company-administered accounts with third-party services providing email, storage, infrastructure, software, data, APIs, business systems, etc., irrespective of whether such accounts are accessed via devices owned/leased by the company or are owned by staff members or a third party.

3. Policy Statement

CNTXT has a culture of trust and integrity. This policy aims to reinforce the trust we place in each other by ensuring we can collectively depend on each other to protect the assets of our staff, company, partners, and customers.

Security is a company-wide effort and requires cooperation from every staff member who works with CNTXT systems. Individuals should take precautions to ensure they use systems appropriately and not deliberately or inadvertently perform destructive or illegal actions.

4. Separation of Concerns

Company-issued devices and accounts are not personal property, so limiting their use for personal reasons is strongly recommended.

5. Security of Critical Data

- All data stored on computing and storage devices, whether owned or leased by CNTXT, the employee, or a third party, remains the sole property of CNTXT.
- You must ensure that all critical data is handled and secured in accordance with the Data Classification Policy.
- You are required to promptly report theft, loss, or unauthorized disclosure of any critical data.
- You may access, use or share critical data only to the extent authorized and necessary to perform your job responsibilities.
- Staff members are responsible for exercising good judgment when using CNTXT systems for reasonable personal use. If there is any uncertainty, staff members must consult their supervisor or manager.
- CNTXT reserves the right to audit any system at any time to ensure compliance with this policy. Authorized individuals within CNTXT may monitor equipment, systems, and network anytime.

6. Unacceptable Use

Staff members may not use CNTXT-managed resources for activities that are illegal or prohibited under applicable law, no matter the circumstances.

6.1 Unacceptable System & Network Activities

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations.
- Unauthorized copying, distribution, or use of copyrighted material.
- Exporting software, technical information, encryption software, or technology in violation of international or national export control laws.
- Intentional introduction of malicious programs into CNTXT networks or any CNTXT-managed computing device.
- Intentional misuse of any CNTXT-managed computing device or CNTXT networks (e.g., for cryptocurrency mining, botnet control, etc.).
- Sharing your credentials for any CNTXT-managed computer or 3rd party service that CNTXT uses with others, or allowing the use of your account or a CNTXT-managed computer by others. This prohibition does not apply to single-sign-on or similar technologies, the use of which is approved. Using a CNTXT computing asset to procure or transmit material that is in violation of sexual harassment policies or that creates a hostile workplace.
- Making fraudulent offers of products, items, or services originating from any CNTXT account. Intentionally accessing data or logging into a computer or account that the team member or contractor is not authorized to access, disrupting network communication, or computer processing or access.

- Executing any form of network monitoring that intercepts data not intended for the team member's or contractor's computer, except when troubleshooting networking issues for the benefit of CNTXT.
- Circumventing user authentication or security of any computer host, network, or account used by CNTXT.
- Tunneling between network segments or security zones, except when troubleshooting issues for the benefit of CNTXT and its customers.

6.2 Unacceptable Email & Communications Activities

- Forwarding confidential business emails or documents to personal external email addresses.
- Note: CNTXT may retrieve messages from archives and servers without prior notice if CNTXT has sufficient reason to do so. If deemed necessary, this investigation shall be conducted with the knowledge of the Information Security Officer, Senior Management, People Business Partners, and the Legal team.

6.3 Return of CNTXT-Owned Assets

All CNTXT owned computing resources should be returned upon separation from the company.

7. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

8. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

9. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

10. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Acceptable Usage Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024