CENTENE® Corporation

End User Security Agreement

This End User Security Agreement outlines and documents your acceptance of the expected behavior for workforce members of Centene Corporation and its subsidiaries. Failure to follow the guidelines and respective policies below may result in disciplinary action up to, and including, termination of employment. Please review carefully before acknowledging.

1. **Passwords:** All users requiring access to our network must have a unique password for each individual network account. Passwords must not be written down, otherwise displayed, or shared with anyone. Password security policies must be followed at all times.

   Policies: CC.SECR.09.03, CC.SECR.09.03.A, CC.SECR.09.04, CC.SECR.09.04.A

2. **Logging Off:** PCs/terminals must be logged off or locked when left unattended. When leaving your desk, users must utilize the Ctrl+Alt+Delete or Windows+L lock functions. When devices and PC monitors are left in the office, they should be left secured, powered on, but logged off overnight to facilitate the installation of software patches. Company-owned computers and laptops must be connected to the company network at least once every 15 days (either by VPN or direct connection at a workplace) to ensure security patches and updates are current.

   Policies: CC.SECR.08.01, CC.SECR.08.01.A, CC.SECR.11.02, CC.SECR.11.02.A

3. **Software:** Only company-approved software may be installed and used on company computers, laptops, or smart phones. Software from outside sources must be assessed and approved before being installed or used. If unauthorized or unlicensed software is found on company-owned hardware, it will be removed immediately.

   Policies: CC.SECR.12.05, CC.SECR.12.05.A, CC.SECR.12.06, CC.SECR.12.06.B, CC.SECR.12.06.B.1

4. **Company Software and Proprietary Information:** Under no circumstances is company-owned software, or restricted / confidential information, to be removed from company systems or copied to any unauthorized system.

   Policies: CC.SECR.08.02, CC.SECR.08.02.A, CC.SECR.08.03, CC.SECR.08.03.A, CC.SECR.14.02, CC.SECR.14.02.B

5. **Hardware:** Users may not connect personal equipment to company equipment or Centene networks without approval. Laptop safeguards are to be used at all times. Cable locks are mandatory for all laptops accessing Centene data.

   Policies: CC.SECR.08.01, CC.SECR.08.01.A, CC.SECR.11.02, CC.SECR.11.02.A

CENTENE® Corporation

End User Security Agreement

(Continued)

6. **External Storage Devices:** External storage devices such as CD-R/W, DVD-R/W, USB storage devices and flash media are prohibited. Centene reserves the right to confiscate and wipe/reformat unauthorized external data storage devices without review or regard for personal content. If external storage devices are critical to specific company operations, users must follow the request and secure-use policies for such devices.
Policies: CC.SECR.08.03, CC.SECR.08.03.A, CC.SECR.08.03.A.1

7. **Protecting Access Credentials:** Credentials used to authenticate to Centene's network and systems are assigned to authorized individuals and must be restricted. If anyone asks you for your credentials or log-in information, the incident must be reported to Report2cyber@centene.com immediately.
Policies: CC.SECR.09.03, CC.SECR.09.03.A, CC.SECR.09.04, CC.SECR.09.04.A, CC.SECR.16.1, CC.SECR.16.1.A

8. **Backups:** The IT Department is responsible for maintaining full network backups. Users should save all work to the Centene network. Local hard drives are to be used only for temporary file swaps and performance-dependent software applications. Users must not store any business-related information on local hard drives.
Policies: CC.SECR.08.01, CC.SECR.08.01.A, CC.SECR.12.03, CC.SECR.12.03.A

9. **Data Sharing / Data Loss Prevention:** Distribution of any Centene data to non-Centene devices or storage mediums is prohibited without proper authorization from company management. These actions include, but are not limited to, forwarding data via email (including to personal email accounts), infrared file passing, or copying data to chat sessions or electronic bulletin boards.
Policies: CC.SECR.13.02, CC.SECR.13.02.A, CC.SECR.13.02.C, CC.SECR.06.02, CC.SECR.06.02.A

10. **Company Equipment / Laptop Protection:** Appropriate care and protection of Centene equipment is required. Negligence in protecting company equipment may result in personal liability to the user. Laptops being transported by vehicle must be kept locked in the trunk or secured out-of-sight. All company devices, software, and systems are company property intended solely for business use. As such, they are subject to inspection, examination, usage monitoring and/or disclosure by authorized company personnel at any time and for any reason. Employees do not have an expectation of privacy on any company device, network or system.
Policies: CC.SECR.08.01, CC.SECR.08.01.A, CC.SECR.11.02, CC.SECR.11.02.A

CENTENE® Corporation

End User Security Agreement

(Continued)

11. **Social Media/Networking sites:** The use of social media/networking sites is prohibited when using a Centene device without proper authorization from Centene management. Posting confidential organizational information or posting on behalf of the company on public websites is prohibited without prior permission. Failure to adhere to the Social Media policy may result in disciplinary action.
Policies: CC.SECR.08.01, CC.SECR.08.01.A, CC.COMM.21

12. **Protection Against Malicious Code:** Employees should use their best judgement to protect Centene, its systems and network from cybercriminals or malicious code. This includes refraining from clicking on suspicious web and email links, navigating to unsecure websites, or opening attachments from unsolicited or phishing emails. All suspicious emails should be reported immediately to Report2Cyber@centene.com.
Policies: CC.SECR.12.02, CC.SECR.12.02.A

13. **Security Incident Reporting:** Any suspected or actual violations of Centene Information Security policy must immediately be reported to Report2Cyber@centene.com.
Policies: CC.SECR.16.01, CC.SECR.16.01.A

14. **Internet and Personal Use of Centene Assets**: Occasional, incidental personal use of Centene provided equipment is acceptable so long as such use does not interfere with the regular conduct of business, does not violate state or federal law, does not violate Centene policy or the Internet Acceptable Use standard (**CC.SECR.08.01.A**), and does not require the installation or use of additional software or peripherals including, but not limited to, removable media.
Policies: CC.SECR.08.01, CC.SECR.08.01.A

15. **Security Policy Compliance**: All users of Centene systems must adhere to the Information Security policies, standards, and procedures. If a security policy violation occurs, Centene must take corrective action, which may include discipline up to, and including, termination of employment.
Policies: CC.SECR.07.01, CC.SECR.07.01.A

16. **Company-Issued Information for Credentials**: Company assigned identifiers must be used when creating or accessing systems used as part of regular business. Registration, or identification to, third parties while conducting business on behalf of Centene must be performed using a Centene provided email address, phone number, and/or mailing address. This includes, but is not limited to, systems owned and maintained by third parties.
Policies: CC.SECR.08.01, CC.SECR.08.01.A