Oxcyon Remote Access Policy

Overview

Oxcyon Inc. (Oxcyon) may permit remote access to its network(s) and system(s) to facilitate productivity and collaboration. Remote access may originate from networks that are compromised or have a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Oxcyon, we must mitigate these external risks to the best of our ability.

Purpose

Oxcyon has put in place the Remote Access Policy (Policy) to define rules and requirements for connecting to Oxcyon Inc.'s network from any device. Oxcyon may potentially be exposed to damages that may result from unauthorized use of Oxcyon resources. Potential damages include loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical Oxcyon internal systems, and fines or other financial liabilities incurred as a result of data loss. Compliance with the Policy is strictly required and necessary to prevent any such losses and damages.

Scope

This policy applies to all Oxcyon's full time and part time employees, independent contractors, temporary and contingent workers, vendors, suppliers and agents or any other business partner (Authorized User) who connects to the Oxcyon's network whether through a company-owned or personally- owned device. This policy also applies to remote access connections used to do work on behalf of Oxcyon Inc. including reading and sending email, accessing applications & intranets and other Oxcyon resources. This policy covers any and all technical implementations of remote access used to connect to the Oxcyon Inc. network. All Authorized Users must adhere to the Policy regardless of the country in which they work.

Policy

It is the responsibility of everyone with remote access privileges to Oxcyon's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Oxcyon.

General access to the Internet for business use through the Oxcyon Inc. network is strictly limited Authorized Users. When accessing the Oxcyon Inc. network from a personal computer, Authorized Users are responsible for preventing access to any Oxcyon Inc. computer resources or data by non- authorized users. Performance of illegal activities through the Oxcyon Inc. network by any user (authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. Authorized Users will not use Oxcyon Inc. networks to access the Internet for outside business interests.

Policy Requirements

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passwords.
- Authorized Users shall protect their login and password, even from family members.
- While using a Oxcyon Inc.-owned computer to remotely connect to Oxcyon Inc.'s corporate network, Authorized Users shall ensure the remote device is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to access the Oxcyon Inc. network must be approved in advance by the appropriate business unit and/or IT management.
- All devices that are connected to Oxcyon Inc. internal networks via remote access technologies must use the most up-to-date anti-virus software and operating system, this includes personal computers. More on device access requirements can be found in the Oxcyon Technical Environment Policies included in this Addendum. For copies of other IT policies contact info@oxcyon.com

Policy Compliance

Oxcyon IT Security will verify compliance with this Policy through various methods, including but not limited to, internal and external audits, and inspection. Feedback will be provided directly to the CIO and the Infrastructure Director. Any exception to the Policy must be approved by the CIO, Oxcyon IT Security or an Infrastructure Director in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any user found in violation of this policy will have their access to Oxcyon network or system revoked.

Revision History

Date of Change	Responsible	Summary of Change
June 2023	Oxcyon Policy Team	Draft Oxcyon's remote access policy

Addendum

Oxcyon Technical Environment Policy for Associates

Overview

Oxcyon Inc. invests a substantia of money to provide its associates and business partners with a robust Technical Environment that includes computers, networks, application software, mobile devices, internet services and access, intranet locations, voice mail, e-mail, copiers, printers, and fax machines. In addition, Oxcyon accommodates the use of personal devices. These capabilities provide Oxcyon a superior Technical Environment to pursue Oxcyon business in a professional and ethical manner.

Scope

This policy applies to all Oxcyon Associates ("Users") who have access to Oxcyon systems, software, equipment and/or data. All Users must adhere to the following policy regardless of the country in which they work.

Purpose

This Oxcyon Technical Environment Policy for Associates ("Policy") broadly addresses the device security, data security, data breach, and use of Social Media.

Policy

1. The Oxcyon Technical Environment is for business purposes only.
2. Users are not permitted to play games, access streaming video or audio, access social media unless specifically approved.
3. Users may not use, store, communicate or access any information that is offensive, vulgar, obscene, pornographic, hateful, illegal, immoral, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of Oxcyon.

4. Users may not use the Oxcyon technical environment to defame anyone, to damage or disparage Oxcyon, its associates, its owners or reputation, nor make or post indecent remarks, proposals, or any offensive, hurtful or discriminatory materials on the Internet.

5. Users are not permitted to solicit, proselytize and/or promote commercial ventures, religious or political causes, outside organizations and other events or causes not sponsored by Oxcyon.

6. Users are not to make any representation of their personal opinion as being that of Oxcyon on the internet, social media or any other electronic means without explicit authorization to do so.

8. Users are not permitted to share passwords or user credentials, nor are they permitted to access, examine, change, or use another person's mailbox, files, view their messages, data or other personal information without explicit authorization.

10. Users should not assume a right of privacy. Oxcyon reserves the right to monitor and access any and all transmissions, communications, data and documents stored within the Oxcyon technical environment.

13. Users may not do anything to damage, delete, overload, interfere with, or otherwise impair the Oxcyon Technical Environment.

14. The Oxcyon technical environment may not be used to infringe on any third party intellectual property rights, or to copy, download, store or forward any third party intellectually protected property or copyrighted materials including audio, video, movies, photographs, graphics, trade secrets or other protected files.

15. Oxcyon technical environment Users are not permitted to download any software or electronic files without seeking assistance or relevant approval from the IT Department.

16. Users must immediately report any misuse of the Oxcyon technical environment to their Supervisor, Oxcyon Legal (info@Oxcyon.com) or to Oxcyon IT (Info@Oxcyon.com).

Device Security

All Devices accessing the Oxcyon technical environment should:

- Device should be password/pass code protected
- Device should utilize up to date anti-virus software
- Device should have up to date operating system
- Device should not be a shared family device
- Device should never be left in an unattended vehicle
- Device should not store Oxcyon business data nor Oxcyon personal data
- Device should securely connect through VPN/RDP

Data Security

Users are required to protect personal information/data that we obtain regarding our associates, customers, contacts, and prospects. While specific laws in each state and province may vary, following are some general data protection principles.

We must use reasonable security procedures and practices to protect personal data from being breached. This includes encryption, redaction, or other protective measures developed by Oxcyon Inc. We can only collect personal information that is reasonable, necessary, and proportionate to achieve our business purpose.

PERSONAL INFORMATION

Any information that identifies, relates to describes, is reasonably capable of being associated with, or could reasonably be linked, with a particular person. For example:

- Name, address, personal identifier, IP address, email address, account names, Social Security number, driver's license number, and passport number.
- Signature, physical characteristics or description, telephone number, education, employment, employment history, and financial account information.
- Some states include commercial information regarding records of personal property, products or services purchased or obtained or considered, or other purchasing history or tendencies.
- Biometric information: physical or behavioral human characteristics to that can be used to digitally identify a person such as fingerprints, facial patterns, or voice.
- Internet or other electronic network activity such as browsing history, search history, and information regarding a person's interaction with a website, application, or advertisement.
- Some states include inferences drawn from any of the information listed above to create a profile about a consumer reflecting the person's preferences, characteristics, psychological trends, behaviors, attitudes, abilities, etc.

Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information collected, transmitted, stored or otherwise processed by Oxcyon Inc..

Access to Oxcyon systems, networks, servers, or devices by an unauthorized entity.

Unauthorized access to and/or distribution of collected personal information of Oxcyon customers, prospects, leads, associates, candidates, applicants, vendors, or agents.

Examples:

- Lost or stolen hardware: Laptops, tablets, phones.
- Lost or stolen agendas, notebooks, address books, etc.
- Computer, tablet, or phone infected with virus or malware.

- Hard copies of documents or files left unattended in the workplace and/or uncollected on a printer or fax machine containing personal data.
- Electronic mail, paper mail, or fax communication containing personal information delivered to the incorrect recipient.
- A direct marketing e-mail sent to recipients visible in the 'to' or 'cc' field enabling each recipient to see the name and/or email address of other recipients.

Use of Social Media

Social Media platforms include, without limitation: Facebook, Linked In, YouTube, Google Video, Twitter, Snap Chat, etc.

DO NOT collect and/or record social media handles or usernames in any Oxcyon database. You may communicate and interact with leads, prospects, and customers within the confines of the social media application while abiding by Oxcyon Inc.'s social media policy. Refrain from personal opinions, disparaging remarks, and professing opinions on behalf of Oxcyon Inc. or any of its business units.

Must adhere to the following:

1. All the rules applicable to the use of Oxcyon technical environment outline above apply to the use of social media.

2. You cannot claim that you are speaking on behalf of Oxcyon Inc. without obtaining approval of the Oxcyon Board, the CIO, the CEO, or the Legal Department.

3. You must not use Oxcyon logos, trademarks or other trade designations without permission.

4. You may not use any content that is owned by and/or copyrighted by third parties, such as graphics, images, movie clips or photographs, etc. without written consent or permission of the author or the rightful owner. A Customer Consent form is available from the Legal Department or the business manager.

5. You may not create You Tube, Google or other videos demonstrating Oxcyon products or services, or make claims about Oxcyon products and services, and post them with Oxcyon logos or corporate markings without the approval of the Oxcyon Board, the CEO or the Legal Department.

6. You cannot use social media to make any claims in writing or verbally about Oxcyon products or services without obtaining the approval of the Oxcyon management team the CEO or the Legal Department.

7. Do not create a social media site, post or video intended to support sales of Oxcyon products or services unless you have approval and specific authority to do so.

8. Do not create social media sites, pages, groups or posts relative to Oxcyon's products, services, platforms or marketing initiatives without obtaining approval from the Legal Department, the CIO or the CEO.

9. You may link and share Oxcyon approved social media sites and their content.

10. When you are participating on social networking sites using your personal social media accounts, clearly state that your thoughts are your own if discussing official Oxcyon business. Use your real identity and disclose your affiliation with Oxcyon. Do not post content that may be disparaging, embarrassing, illegal, or potentially harming to Oxcyon's business or reputation.

11. Do not engage with the news media or industry analysts to discuss business on Oxcyon's behalf unless you have approval or are authorized to do so as a representative of the company.

Policy Questions

All questions about this Policy or any other areas regarding Information Technology should be directed to the Chief Information Officer (CIO), who can be contacted at mkerchenski@oxcyon.com

Revision History

Oct 2022	Oxcyon Policy Team	Draft Oxcyon's associate Technical Environment policy
Oct 2023	Oxcyon Policy Team	Policy revisions to align with the contractor 2020 policy

Oxcyon Technical Environment Policy for Contractors

Overview

Oxcyon Inc. invests a substantial amount of money to provide its associates and business partners with a robust Technical Environment that includes computers, networks, application software, mobile devices, internet services and access, intranet locations, voice mail, e-mail, copiers, printers, and fax machines. In addition, Oxcyon accommodates the use of personal devices. These capabilities provide Oxcyon a superior Technical Environment to pursue Oxcyon business in a professional and ethical manner.

Scope

This policy applies to all Oxcyon business partners, including without limitation, independent sales agents, brokers, contractors, temporary and contingent workers, vendors, suppliers, consultants ("Users") who have access to Oxcyon systems, software, equipment and/or data. All Users must adhere to the following policy regardless of the country in which they work.

Purpose

This Oxcyon Technical Environment Policy for Contractors ("Policy") broadly addresses the device security, data security, data breach, and use of Social Media.

Policy

1. The Oxcyon Technical Environment is for business purposes only.

2. Users are not permitted to play games, access streaming video or audio, access social media unless specifically approved.

3. Users may not use, store, communicate or access any information that is offensive, vulgar, obscene, pornographic, hateful, illegal, immoral, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of Oxcyon.

4. Users may not use the Oxcyon technical environment to defame anyone, to damage or disparage Oxcyon, its associates, its owners or reputation, nor make or post indecent remarks, proposals, or any offensive, hurtful or discriminatory materials on the Internet.

5. Users are not permitted to solicit, proselytize and/or promote commercial ventures, religious or political causes, outside organizations and other events or causes not sponsored by Oxcyon.

6. Users are not to make any representation of their personal opinion as being that of Oxcyon on the internet, social media or any other electronic means without explicit authorization to do so.

7. Users are not permitted to share passwords or user credentials, nor are they permitted to access, examine, change, or use another person's mailbox, files, view their messages, data or other personal information without explicit authorization.

8. Users should not assume a right of privacy. Oxcyon reserves the right to monitor and access any and all transmissions, communications, data and documents stored within the Oxcyon technical environment.

9. Users may not do anything to damage, delete, overload, interfere with, or otherwise impair the Oxcyon technical environment.

10. The Oxcyon technical environment may not be used to infringe on any third party intellectual property rights, or to copy, download, store or forward any third party intellectually protected property or copyrighted materials including audio, video, movies, photographs, graphics, trade secrets or other protected files.

Oxcyon technical environment Users are not permitted to download any software or electronic files without seeking assistance or relevant approval from the IT Department.

11. Users must immediately report any misuse of the Oxcyon technical environment to their Supervisor, Oxcyon Legal (info@Oxcyon.com) or Oxcyon IT (production@oxcyon.com).

12. Users should not open email from unknown sources, nor should they open or click on any suspicious links embedded in a website or email.

13. Users should never open or respond to emails asking for passwords, money, access to bank or personnel data or access to Oxcyon systems.

14. Users should never access personal email, cloud file shares, etc. while on Oxcyon's technical environment.

Device Security

All Devices accessing the Oxcyon technical environment should:

- Device should be password/pass code protected
- Device should utilize up to date anti-virus software
- Device should have up to date operating system
- Device should not be a shared family device
- Device should never be left in an unattended vehicle
- Device should not store Oxcyon business data nor Oxcyon personal data
- Device should securely connect through Oxcyon's Cisco AnyConnect VPN

Data Security

Users are required to protect personal information/data that we obtain regarding our associates, customers, contacts, and prospects. While specific laws in each state and province may vary, following are some general data protection principles.

We must use reasonable security procedures and practices to protect personal data from being breached. This includes encryption, redaction, or other protective measures developed by Oxcyon Inc.. We can only collect personal information that is reasonable, necessary, and proportionate to achieve our business purpose.

PERSONAL INFORMATION

Any information that identifies, relates to describes, is reasonably capable of being associated with, or could reasonably be linked, with a particular person. For example:

- Name, address, personal identifier, IP address, email address, account names, Social Security number, driver's license number, and passport number.

- Signature, physical characteristics or description, telephone number, education, employment, employment history, and financial account information.
- Some states include commercial information regarding records of personal property, products or services purchased or obtained or considered, or other purchasing history or tendencies.
- Biometric information: physical or behavioral human characteristics to that can be used to digitally identify a person such as fingerprints, facial patterns, or voice.
- Internet or other electronic network activity such as browsing history, search history, and information regarding a person's interaction with a website, application, or advertisement.
- Some states include inferences drawn from any of the information listed above to create a profile about a consumer reflecting the person's preferences, characteristics, psychological trends, behaviors, attitudes, abilities, etc.

Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information collected, transmitted, stored or otherwise processed by Oxcyon Inc..

Access to Oxcyon systems, networks, servers, or devices by an unauthorized entity.

Unauthorized access to and/or distribution of collected personal information of Oxcyon customers, prospects, leads, associates, candidates, applicants, vendors, or agents.

Examples:

- Lost or stolen hardware: Laptops, tablets, phones.
- Lost or stolen agendas, notebooks, address books, etc.
- Computer, tablet, or phone infected with virus or malware.
- Hard copies of documents or files left unattended in the workplace and/or uncollected on a printer or fax machine containing personal data.
- Electronic mail, paper mail, or fax communication containing personal information delivered to the incorrect recipient.
- A direct marketing e-mail sent to recipients visible in the 'to' or 'cc' field enabling each recipient to see the name and/or email address of other recipients.

Use of Social Media

Social Media platforms include, without limitation: Facebook, Linked In, YouTube, Google Video, Twitter, Snap Chat, etc.

DO NOT collect and/or record social media handles or usernames in any Oxcyon database. You may communicate and interact with leads, prospects, and customers within the confines of the social media application while abiding by Oxcyon Inc.'s social media policy. Refrain from personal opinions, disparaging remarks, and professing opinions on behalf of Oxcyon Inc. or any of its business units.

Policy Questions

All questions about this Policy or any other areas regarding Information Technology should be directed to the Chief Information Officer (CIO), who can be contacted at mkerchenski@oxcyon.com

Revision History

June23	Oxcyon Policy	Draft Oxcyon's contractor Technical Environment

By typing your name below, you hereby acknowledge that this Policy does not create an employment, fiduciary, partnership or other special relationship between Oxcyon and users not currently employed by Oxcyon. Any such external user will not be eligible for any employment benefits, compensation or remuneration on the basis of being construed as an employee.

Please send signed policies to mkerchenski@oxcyon.com

Company Name (if different than Oxcyon): _____

Name: _____

Date: _____