FRAXION

IT security policy

Information technology security policy

T: 206-256-0771

1000 Second Avenue
Suite 2500
Seattle, WA 98104

info@fraxion.biz
fraxion.biz

Table of contents

General policy

1.1 Context

Fraxion aspires to a Zero Trust Security Architecture, pervasive across all systems, applications, and hardware. This includes all resources, internal, external, cloud hosted, used by internal staff, customers or partners.

Zero trust Architecture is defined by Microsoft as:

Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify." Every access request is fully authenticated, authorized, and encrypted before granting access. Micro segmentation and least privileged access principles are applied to minimize lateral movement. Rich intelligence and analytics are utilized to detect and respond to anomalies in real time. Ref: Microsoft Zero Trust

Further reading: Wikipedia

1.2 Purpose

This security policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in Fraxion. Its goal is to protect Fraxion its employees and IT users, customers, and data to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

1.3 Scope

This document applies to all the users in Fraxion, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency.

1.4 History

Version	Description	From	To	Author
1.0	Initial version	8/1/2021		Mark du Plessis
1.1	Joe and Eric input integrated.	9/9/2021		Joe, Hansen, Eric Cisco, Mark du Plessis

1.2	Data security and privacy	9/16/2021	John O'Callaghan
1.3	Comments	9/16/2021	Mark du Plessis
1.5	Final comments	1/7/2022	Mark du Plessis

1.5 Responsibilities

Roles	Responsibilities
Chief Executive Officer	Accountable for all aspects of Fraxion's security and integrity.
Information Security Officer	Accountable for all aspects of Fraxion's information security.
Information Technology Manager	Responsible for the security of the IT infrastructure. Plan against security threats, vulnerabilities, and risks. Implement and maintain Security Policy documents. Ensure security training programs. Ensure IT infrastructure supports Security Policies. Respond to information security incidents. Help in disaster recovery plans.
Information Owners	Help with the security requirements for their specific area. Determine the privileges and access rights to the resources within their areas.
IT Security Team	Implements and operates IT security. Implements the privileges and access rights to the resources. Supports Security Policies.
Users	Meet Security Policies. Report any attempted security breaches.

1.6 General policy definitions

1. Exceptions to the policies defined in any part of this document may only be authorized by the Information Security Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
2. All IT services should be used in compliance with the technical and security requirements defined in the design of the services.
3. Infractions of the policies in this document may lead to disciplinary actions. In some serious cases they could even lead to prosecution.
4. This document should be read in conjunction with the Fraxion Data and Privacy Policy and the Fraxion Data Security Program.

Acceptable use policy

Purpose

The purpose of this policy is to outline the acceptable use of the Fraxion network and Fraxion computer resources. These rules are in place to protect authorized users and Fraxion. Inappropriate use exposes Fraxion to risks including virus attacks, compromise of network systems and services, compromise of Fraxion or Fraxion customer data, and legal issues.

Scope

This policy applies to the use of information, computers, electronic devices, and network resources used to conduct Fraxion business, as well as any device that interacts with Fraxion internal and external networks, business systems, products and services, whether hosted externally or on premises, owned or leased by Fraxion, the employee, or a third party. All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at Fraxion, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Fraxion policies and standards, local laws, and regulations.

Policy definitions

Ownership of electronic files

All electronic files created, sent, received, or stored on Fraxion owned, leased, or administered equipment or otherwise under the custody and control of Fraxion are the property of Fraxion.

Privacy

Electronic files created, sent, received, or stored on Fraxion owned, leased, or administered equipment, or otherwise under the custody and control of Fraxion are not private and may be accessed by Fraxion IT employees at any time without knowledge of the user, sender, recipient, or owner.

Electronic file content may also be accessed by appropriate personnel in accordance with directives from Human Resources or the CEO.

General use and ownership

Access requests must be authorized and submitted from departmental supervisors for employees to gain access to computer systems. Authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that the data and files they create on the corporate systems immediately become the property of Fraxion. Because of the need to protect Fraxion's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to Fraxion.

For security and network maintenance purposes, authorized individuals within the Fraxion IT Department may monitor equipment, systems, and network traffic at any time.

Fraxion's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Fraxion's IT Department reserves the right to remove any non-business related software or files from any system.

Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

System level and user level passwords must comply with the Password Policy. Authorized users must not share their Fraxion login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes with any other party, inside or outside of the company.

Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Authorized users may access, use, or share Fraxion proprietary information only to the extent it is authorized and necessary to fulfill the users assigned job duties.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less.

All users must lockdown their PCs, laptops, and workstations by locking (control-alt- delete) when the host will be unattended for any amount of time. For servers and on-premises workstations, employees must log-off, or restart (but not shut down) their PC after their shift.

Fraxion proprietary information stored on electronic and computing devices, whether owned or leased by Fraxion, the employee, or a third party, remains the sole property of Fraxion. All proprietary information must be protected through legal or technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of Fraxion proprietary information to their immediate supervisor and/or the IT Department.

All users must report any weaknesses in Fraxion computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the IT Department.

Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes. Users should report suspicious messages as instructed by IT staff.

Unacceptable use

Users must not intentionally access, create, store, or transmit material which Fraxion may deem to be offensive, indecent, or obscene.

Under no circumstances is any individual associated in any way with Fraxion authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Fraxion-owned resources.

System and network activities

The following activities are prohibited by users, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Fraxion.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Fraxion or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to IT.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using a Fraxion computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
6. Attempting to access any data, electronic content, or programs contained on Fraxion systems for which they do not have authorization, explicit consent, or implicit need for their job duties.
7. Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of Fraxion IT.
8. Installing or using non-standard shareware or freeware software without Fraxion IT approval.
9. Installing, disconnecting, or moving any Fraxion owned computer equipment and peripheral devices without prior consent of Fraxion's IT Department.
10. Purchasing software or hardware, for Fraxion use, without prior IT compatibility review.
11. Purposely engaging in activity that may:
    - degrade the performance of information systems

- deprive an authorized Fraxion user access to a Fraxion resource
- obtain extra resources beyond those allocated
- circumvent Fraxion computer security measures

12. Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, Fraxion users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on Fraxion information systems. The Fraxion IT Department is the only department authorized to perform these actions.
13. Circumventing user authentication or security of any host, network, or account.
14. Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Access to the Internet at home, from a Fraxion-owned computer, must adhere to all the same policies that apply to use from within Fraxion facilities. Authorized users must not allow family members or other non-authorized users to access Fraxion computer systems.
17. Fraxion information systems must not be used for personal benefit.

Incidental use

As a convenience to the Fraxion user community, incidental use of information systems is permitted. The following restrictions apply:

1. Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.
2. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to Fraxion approved users; it does not extend to family members or other acquaintances.
3. Incidental use must not result in direct costs to Fraxion without prior approval of management.
4. Incidental use must not interfere with the normal performance of an employee's work duties.
5. No files or documents may be sent or received that may cause legal action against, or embarrassment to, Fraxion.
6. Storage of personal email messages, voice messages, files, and documents within Fraxion's information systems must be nominal.
7. All messages, files, and documents — including personal messages, files, and documents — located on Fraxion information systems are owned by Fraxion, may be subject to open records requests, and may be accessed in accordance with this policy.

IT assets policy

Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in Fraxion.

Scope

The policy applies to servers, network devices, desktops, mobile devices, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

Policy definitions

1. IT assets must only be used in connection with the business activities they are assigned and / or authorized.
2. All the IT assets must be classified into one of the categories in Fraxion's security categories; according to the current business function they are assigned to.
3. Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
4. All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.
5. Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.
6. Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.
7. All personnel interacting with the IT assets must have the proper training.
8. Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
9. Access to assets in Fraxion locations must be restricted and properly authorized, including those accessing remotely. Company's laptops, phones, tablets, and any other computer, network, or communications equipment used at an external location must be periodically checked and maintained.
10. The IT Technical Teams are the sole responsible parties for maintaining and upgrading configurations. No other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
11. Special care must be taken for protecting laptops and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields, liquids, and falls.
12. When travelling by plane, portable equipment such as laptops, communication devices, other computing equipment, and data-storage devices must remain in possession of the user as hand luggage.
13. Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen.
14. Losses, theft, damages, tampering, or other incident related to assets that compromises security must be reported as soon as possible to the Information Security Officer.
15. Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an

Information Security Team member. Assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

Access control policy

Purpose

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in Fraxion. The access control policy and principles of least privilege are fundamental underpinning features of Fraxion's Zero Trust Architecture.

Scope

This policy applies to all the users in Fraxion, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Fraxion hosts products and services on behalf of its customers. These systems store and manage data private to customers. This data is specifically highly confidential, and all policies apply strictly thereto.

Policy definitions

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Any system that handles confidential information must be protected by a two factor -based access control system.
3. Discretionary access control list must be in place to control the access to resources for different groups of users.
4. Mandatory access controls should be in place to regulate access by process operating on behalf of users.
5. Access to resources should be granted on a per-group basis rather than on a per-user basis, as a general principle.
6. Access shall be granted under the principle of “less privilege”, i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform their business functions successfully.
7. Whenever possible, access should be granted through centrally defined and centrally managed identities.
8. Users should in no circumstances tamper with or evade the access control in order to gain greater access than they are assigned.
9. Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.

Password control policy

Purpose

The Password Control Policy section defines the requirements for the proper and secure handling of passwords in Fraxion.

Scope

This policy applies to all the users in Fraxion, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy definitions

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Every user must have a separate, private identity for accessing IT network services.
3. Identities should be centrally created and managed. Single sign-on for accessing multiple services should be used wherever possible.
4. Each identity must have a strong, private, and unique alphanumeric password to be able to access any service. Employees should not use common or known compromised passwords. Multi-factor authentication should be used whenever possible.
5. Password for some special identities must be at least 15 characters long.
6. Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two set of credentials: one for administrative work and the other for common work.
7. Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
8. Whenever a password is deemed compromised, it must be changed immediately.
9. For critical applications, digital certificates and multiple factor authentication using smart cards should be used whenever possible.
10. Identities must be locked if password guessing is suspected on the account.

Email policy

Purpose

The Email Policy section defines the requirements for the proper and secure use of electronic mail in Fraxion.

Scope

This policy applies to all the users in Fraxion, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy definitions

1. All Fraxion assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of Fraxion.
2. Occasional use of personal email address on the Fraxion network for personal purposes may be permitted if in doing so there is no perceptible consumption in Fraxion system resources and the productivity of the work is not affected.
3. Use of Fraxion resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to Fraxion business is strictly forbidden.
4. In no way may the email resources be used to reveal confidential or sensitive information from Fraxion outside the authorized recipients for this information.

5. Using the email resources of Fraxion for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law is forbidden.
6. Use of Fraxion email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
7. Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriated.
8. Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged. However, only the Information Security Officer may approve the interception and disclosure of messages.
9. Identities for accessing corporate email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the company's procedures for managing identities. Sharing of passwords is discouraged. Users may not impersonate another user.
10. Outbound messages from corporate users should have approved signatures at the foot of the message.
11. Attachments must be limited in size according to the specific procedures of Fraxion. Whenever possible, restrictions should be automatically enforced.
12. Whenever possible, the use of Digital Rights technologies is encouraged for the protection of contents.
13. Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
14. Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.
15. Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT Continuity Management.

Internet policy

Purpose

The Internet policy section defines the requirements for the proper and secure access to Internet.

Scope

This policy applies to all the users in Fraxion, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy definitions

1. Limited access to Internet is permitted for all users.
2. The use of messaging services is permitted for business purposes.
3. Access to pornographic sites, hacking sites, and other risky sites is strongly discouraged.
4. Downloading is a privilege assigned to some users. It can be requested as a service.

5. Internet access is mainly for business purpose. –some limited personal navigation is permitted if in doing so there is no perceptible consumption of Fraxion system resources, and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
6. Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back-to-back configuration is strongly recommended for firewalls.
7. In accessing Internet, users must behave in a way compatible with the prestige of Fraxion. Attacks like denial of service, spam, phishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
8. Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the Information Security Officer.
9. Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

Antivirus policy

Purpose

The Antivirus policy section defines the requirements for the proper implementation of antivirus and other forms of protection in Fraxion.

Scope

This policy applies to servers, workstations and equipment in Fraxion, including portable devices like laptops and PDA that may travel outside of Fraxion facilities. Some policies apply to external computers and devices accessing the resources of Fraxion.

Policy definitions

1. All computers and devices with access to Fraxion network must have an antivirus client installed, with real-time protection.
2. All servers and workstations owned by Fraxion or permanently in use in Fraxion facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connects to Fraxion network or that can be managed via secure channels through Internet.
3. Organization's computers permanently working in other Organization's network may be exempted from the previous rule if required by the Security Policies of the other Organization, provided those computers will be protected too.
4. Traveling computers from Fraxion that seldom connect to Fraxion network may have installed an approved antivirus independently managed.
5. All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
6. Visitors' computers and all computers that connect to Fraxion's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

Information classification policy

Purpose

The Information classification policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality, and availability of Fraxion information.

Scope

This policy applies to all the information created, owned, or managed by Fraxion, including customers own data, and including those stored in electronic or magnetic forms and those printed in paper.

Policy definitions

1. Customer data, whether retained as part of Fraxion's business processes, or hosted within Fraxion's products and services, automatically qualifies as extremely sensitive and highly confidential.
2. Information owners must ensure the security of their information and the systems that support it.
3. Information Security Management is responsible for ensuring the confidentiality, integrity and availability of Fraxion's assets, information, data and IT services.
4. Any breach must be reported immediately to the Information Security Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.
5. Information in Fraxion is classified according to its security impact. The current categories are confidential, sensitive, shareable, public and private.
6. Information defined as confidential has the highest level of security. Only a limited number of persons must have access to it. Management, access, and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.
7. Information defined as sensitive must be handled by a greater number of persons. It is needed for the daily performing of jobs duties, but should not be shared outside of the scope needed for the performing of the related function.
8. Information defined as shareable can be shared outside of the limits of Fraxion, for those clients, organizations, regulators, etc. who acquire or should get access to it.
9. Information defined as public can be shared as public records, e.g. content published in the company's public Web Site.
10. Information is classified jointly by the Information Security Officer and the Information Owner.

Remote access policy

Purpose

The remote access policy section defines the requirements for the secure remote access to Fraxion's internal resources.

Scope

This policy applies to the users and devices that need access Fraxion's internal resources from remote locations.

Policy definitions

1. To gain access to Fraxion internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
2. Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates.
3. Users must not connect from public computers unless the access is for viewing public content. (I.e., does not require connection to the Fraxion domain or Internal systems.)

Outsourcing policy

Purpose

The Outsourcing policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions, and processes.

Scope

This policy applies to Fraxion; the services providers to whom IT services, functions or processes are outsourced, and the outsourcing process itself.

Policy definitions

1. Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
2. Whenever possible, a bidding process should be followed to select between several service providers.
3. In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
4. Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If Fraxion has not enough knowledge and resources, a specialized company should be hired to do the auditing.
5. A service contract and defined service levels must be agreed between Fraxion and the service provider.
6. The service provider must get authorization from Fraxion if it intends to hire a third party to support the outsourced service, function or process.

Extranet policy

Purpose

This document describes the policy under which third party organizations connect to Fraxion networks for the purpose of transacting business related to Fraxion.

Scope

Connections required by third parties that require access to non-public Fraxion resources fall under this policy, regardless of connection type.

Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for Fraxion, or to the Public Switched Telephone Network, do NOT fall under this policy.

Policy definitions

All new extranet connectivity will go through a security review with the IT Security Team. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principles of zero trust and least privilege are followed.

All new connection requests between third parties and Fraxion require that the third party and Fraxion representatives agree to and sign the Third Party Agreement. This agreement must be signed by the Sponsoring Organization as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the IT Security Team. Documents pertaining to connections into Fraxion lab, test, or demonstration environments are to be kept on file with the responsible team.

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by an overseeing manager. Lab and test environment connections must be approved by the IT Security Team. Typically, this will be handled as part of the overarching Third Party Agreement.

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization and is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the point of contact changes, the IT Security Team must be informed promptly.

Sponsoring Organizations within Fraxion that wish to establish connectivity to a third party are to file a new site request with the IT Security Team. The IT Security Team will work to address security issues inherent in the project. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the IT Security Team as requested. All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review.

All changes in access must be accompanied by a valid business justification and are subject to security review. The Sponsoring Organization is responsible for notifying the IT Security Team when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

When access is no longer required, the Sponsoring Organization within Fraxion must notify the IT Security Team, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The IT Security Team must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct Fraxion business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct Fraxion business necessitate a modification of existing permissions, or termination of connectivity, the IT Security Team will notify the POC or the Sponsoring Organization of the change prior to taking any action.

Policy compliance

The IT Security Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the Information Security Officer in advance.

An employee found to have violated this policy may be subject to disciplinary action.

A third party found to have violated this policy may be subject to termination of agreements or legal action as appropriate.

Annex

Glossary

Term	Definition
Access management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.

Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External service provider	An IT service provider that is part of a different organization from its customer.
Identity	A unique name that is used to identify a user, person, or role.
Information security policy	The policy that governs Fraxion's approach to information security management
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm, loss, or affect the ability to achieve objectives.
Service level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.