Chameleon
Security

Acceptable Use Policy

Definitions

Technology resources: Refers to all computing devices, software applications, network infrastructure, internet access, email services, and any other resources provided by Chameleon Company for business purposes.

Users: Refers to employees, contractors, consultants, vendors, partners, and any other authorized individuals who have been granted access to Chameleon Company's technology resources to conduct business activities.

Sensitive information: Includes, but is not limited to, trade secrets, customer data, financial information, personally identifiable information (PII), internal communications, intellectual property, and any other confidential or proprietary information related to Chameleon Company's business operations.

Unauthorized access: Any attempt to gain access to data or systems without proper authorization, including but not limited to hacking, phishing, exploiting system vulnerabilities, or using someone else's credentials without consent.

Overview

Chameleon Company provides technology resources to support its business operations and enable efficient communication among employees, contractors, vendors, and partners. These resources include a wide range of tools and systems such as computing devices, software applications, network infrastructure, internet access, and email services. By leveraging technology, Chameleon Company aims to streamline workflows, increase productivity, and enhance collaboration across departments and teams.

The technology resources provided by Chameleon Company are essential for conducting day-to-day business activities, including managing projects, communicating with clients, analyzing data, and facilitating internal operations. These resources are designed to empower employees to work effectively and efficiently, whether in the office, remotely, or while traveling for business purposes. Additionally, the technology infrastructure enables seamless integration of business processes, data sharing, and access to critical systems, ensuring a smooth and uninterrupted workflow for all users.

Chameleon Company recognizes the importance of utilizing modern technology to remain competitive in the market, provide high-quality products and services, and meet the evolving needs of its customers. Therefore, the company invests in state-of-the-art technology resources, software solutions, and security measures to safeguard its digital assets, protect sensitive information, and uphold the trust of clients and partners. By adhering to best practices in technology management and information security, Chameleon Company aims to maintain a

secure and reliable environment for its users to conduct business activities effectively and securely.

As technology continues to evolve and play a crucial role in business operations, Chameleon Company remains committed to providing its employees and authorized users with the necessary tools, resources, and support to control technology effectively and responsibly. The company values innovation, efficiency, and security in its technology infrastructure and expects all users to adhere to the guidelines outlined in this Acceptable Use Policy to ensure the proper use, protection, and maintenance of its technology resources.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Chameleon Company. These rules are in place to protect the authorized user and Chameleon Company. Inappropriate use exposes Chameleon Company to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to all users of Chameleon Company's technology resources, including employees, contractors, consultants, vendors, partners, and any other authorized individuals. It encompasses all computing devices, software applications, network infrastructure, internet access, email services, and any other resources provided by Chameleon Company for business purposes. Users are expected to adhere to the guidelines outlined in this policy while accessing, using, or interacting with any of the company's technology resources, regardless of their location or method of access.

Furthermore, this policy extends to the protection of sensitive information, including trade secrets, customer data, financial information, personally identifiable information (PII), internal communications, and intellectual property. Users are required to uphold the confidentiality, integrity, and security of this sensitive information while utilizing Chameleon Company's technology resources. Any unauthorized access, sharing, or disclosure of sensitive information is strictly prohibited and may result in disciplinary action, up to and including termination of employment. Users are responsible for ensuring the proper handling and safeguarding of sensitive information by this policy and applicable laws and regulations.

Ownership of Electronic Files

All electronic files, data, documents, and information created, stored, or transmitted using Chameleon Company's technology resources are considered the property of the company. Users should be aware that the company reserves the right to access, monitor, and review any electronic files or communications stored on its systems for security, compliance, or business purposes. Employees may not delete, modify, or share electronic files without proper

authorization, and are expected to use technology resources in a manner consistent with company policies and guidelines.

Privacy

Chameleon Company values the privacy and confidentiality of its users' personal information and communication. The company will make every effort to protect the privacy of users' data and will not disclose or share personal information without proper consent, except when required by law or for business operations. Users are encouraged to be mindful of the privacy implications of their online activities, interactions, and communications while using Chameleon Company's technology resources, and to report any concerns regarding privacy violations to the appropriate authorities within the company.

General Use and Ownership:

Chameleon Company's technology resources are provided for business purposes and are intended to support the company's operations, projects, and communications. Employees are expected to use technology resources responsibly, ethically, and in compliance with company policies, industry standards, and applicable laws and regulations. Users are prohibited from using technology resources for personal gain, illegal activities, harassment, or any other unauthorized or unethical purposes. Additionally, users should not install unauthorized software, access inappropriate websites, or engage in activities that may compromise the security or integrity of Chameleon Company's technology infrastructure. Users are responsible for maintaining the proper use and ownership of technology resources and are encouraged to seek guidance from the IT department or management if they have any questions or concerns regarding their usage.

Security and Proprietary Information

Chameleon Company is committed to maintaining a secure and confidential environment for all sensitive and proprietary information stored and transmitted through its technology resources. The company recognizes the importance of safeguarding its intellectual property, trade secrets, customer data, financial information, and other confidential data from unauthorized access, disclosure, or misuse.

To ensure the security of proprietary information,

- Chameleon Company utilizes a multi-layered security strategy to protect its proprietary information, including network security measures like firewalls and encryption techniques.
- Access controls are strictly enforced, with user permissions based on the principle of least privilege to limit access to only necessary individuals.

- Regular access reviews are conducted to monitor and adjust user permissions as needed, reducing the risk of unauthorized access to proprietary data.
- Employee training on security best practices, data handling procedures, and the importance of protecting proprietary information is provided to all staff members.
- Partnerships with third-party vendors and service providers who adhere to stringent security standards ensure the secure treatment of proprietary information shared with them.
- Contractual agreements are established with vendors outlining security requirements, data handling practices, and confidentiality obligations.
- Continuous evaluation and enhancement of security measures, strict access controls, ongoing training and awareness programs, and a culture of security consciousness help Chameleon Company maintain the trust and confidence of clients, partners, and stakeholders in safeguarding proprietary information.

Unacceptable Use

- Unauthorized access: Any attempt to access or use systems, networks, or data without proper authorization is strictly prohibited. This includes trying to bypass security measures, use someone else's login credentials, or gain access to information that is not relevant to one's job responsibilities.
- Data manipulation: Any unauthorized alteration, deletion, or addition of data within Chameleon Company's systems or networks is considered a violation of the company's policies. This includes maliciously modifying records, changing settings, or tampering with information stored in databases.
- Malware and malicious software: Intentionally introducing viruses, worms, Trojan horses, ransomware, or other types of malicious software into Chameleon Company's systems or networks is strictly prohibited. This includes downloading unauthorized software or files that could compromise the security of company information.
- Phishing and social engineering: Engaging in activities that attempt to deceive or manipulate employees into revealing sensitive information, such as login credentials, passwords, or financial data, is considered unacceptable. This includes sending fraudulent emails, texts, or calls pretending to be a trusted source in order to trick individuals into divulging confidential information.
- Unauthorized sharing of sensitive information: Disclosing proprietary or confidential information to unauthorized individuals or outside parties without proper authorization is strictly prohibited. This includes sharing trade secrets, client details, financial information, or any other sensitive data without the necessary permissions.
- Misuse of company resources: Using company resources, such as computers, networks, software, or hardware, for personal gain, illegal activities, or any purpose unrelated to work responsibilities is considered unacceptable. This includes excessive personal

internet usage, downloading unauthorized files, or installing unapproved software on company devices.

- Violation of intellectual property rights: Engaging in activities that infringe upon the intellectual property rights of others, such as unauthorized use of copyrighted materials or software, is strictly prohibited. This includes making illegal copies of software, music, videos, or other copyrighted content without the necessary permissions.

These are just a few examples of unacceptable use of company resources and information. Chameleon Company takes these violations seriously and enforces strict policies and measures to maintain the security and confidentiality of its proprietary information. Employees are expected to adhere to these policies and report any suspected breaches or incidents of unauthorized use to the appropriate authorities.

Acceptable Use

Users of Chameleon Company's technology resources should adhere to the following guidelines:

- All users are expected to use company-provided technology resources for business-related tasks only.
- Users should not engage in any activities that could negatively impact the security, integrity, or performance of company systems or networks.
- Users are not permitted to access, upload, download, or distribute any illegal, offensive, or inappropriate content.
- Users should not share their login credentials or access company systems on behalf of unauthorized individuals.
- Users are responsible for protecting their devices from malware and viruses by installing approved security software.
- Users must respect the privacy rights of others and should not access or disclose confidential information without proper authorization.

Prohibited Activities

The following activities are strictly prohibited on Chameleon Company's technology resources:

- Engaging in any form of hacking, unauthorized access, or attempting to circumvent security measures.
- Sharing sensitive company information with unauthorized individuals or entities.
- Using company technology resources for personal gain or conducting personal business activities.

- Engaging in any form of harassment, discrimination, or other inappropriate behavior towards others.
- Engaging in any activities that violate local, state, or federal laws.

Enforcement

Violation of this Acceptable Use Policy may result in disciplinary action, up to and including termination of employment. Chameleon Company reserves the right to monitor and audit employee use of technology resources to ensure compliance with this policy.

Incidental Use

- Incidental personal use of company resources: Employees may engage in occasional and limited personal use of company resources, such as computers, internet access, and email, for personal matters. This includes checking personal emails during breaks, browsing non-work-related websites during downtime, or making personal phone calls during breaks or lunchtime. However, this personal use should be minimal, not interfere with work responsibilities or productivity, and not consume excessive resources.
- Social media use: Employees may use company devices or networks to access social media platforms for personal use during non-work hours or breaks. This may involve checking social media accounts, posting updates, or engaging in personal communications. However, employees are expected to exercise discretion, follow company policies regarding acceptable use of social media, and ensure that their personal activities do not compromise the security of company information or networks.
- Personal device connectivity: In some cases, employees may need to connect their personal devices, such as smartphones or tablets, to company networks or systems for work-related purposes. This could include accessing work emails, documents, or applications on personal devices to complete tasks or stay connected while away from the office. However, employees should ensure that their personal devices meet security requirements, such as having up-to-date antivirus software and encryption settings, to protect company data from potential risks.
- Personal storage and backups: Employees may use company resources to store personal files or data, such as photos, documents, or other personal information, as long as it does not interfere with work-related activities or consume excessive storage space. This could include saving personal files on company servers or using company backup systems to secure personal data. However, employees should be mindful of company policies regarding data storage, backups, and security, and ensure that their personal files do not pose a risk to confidential company information.
- Internet browsing and research: Employees may utilize company resources, such as internet access and research tools, for personal purposes, such as online shopping,

research, or entertainment, during non-work hours or breaks. This incidental use of company resources should be appropriate, legal, and not violate company policies or compromise network security. Employees should be mindful of their browsing habits, avoid accessing inappropriate or potentially harmful websites, and ensure that their personal activities do not interfere with work duties or productivity.

Chameleon Company acknowledges that incidental personal use of company resources may occur and does not prohibit employees from engaging in reasonable and responsible personal activities during appropriate times. However, employees are expected to use good judgment, adhere to company policies and guidelines, and prioritize work responsibilities while utilizing company resources for personal purposes.