Acceptable Usage Policy

Version 2.0

Revision History

Version #	Date (DD-MMM-YYYY)	Details of the Changes	Modified By	Reviewed & Approved By
1.0	17-July-2020	First Release	Vipul Sharma	Vivek Jha
2.0	15-June-2023	Second Release Changes made in point no. 2.3 Laptop/Desktop System Usage	Usha Pattyam	Vivek Jha

Contents

1 Purpose and Scope

1.1 Overview

- Chief Information Security Officer (CISO)'s intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to **DataGain's** established culture of openness, trust and integrity.
- CISO is committed to protecting **DataGain's** employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, exposing to risks including virus attacks, compromise of network systems and services.
- All computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of **DataGain**.
- These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

1.2 Purpose

- This policy addresses **DataGain's** intent to safeguard computing resources from Internet and email-based threats.
- This policy shall underline appropriate user etiquette for workstation, Internet and email usage and define procedures for safeguards from Internet and email borne threats.
- This policy aims to be a concise document intended to be distributed to all **DataGain** employees.
- The purpose of this policy is to outline the acceptable use of computer equipment at **DataGain**.
- These rules are in place to protect the employee and **DataGain**.

1.3 Scope

- This Policy applies to all Employees, Contractors, Vendors, Employees of Third Parties associated with **DataGain** and Consultants having business relationships with **DataGain**.
- This policy covers logical and physical boundaries of **DATAGAIN**.
- This policy covers all **DataGain's** network, Operations area, IT systems, data and authorized users, public users within logical and physical boundaries.

2 Policy Standards

2.1 General use and Ownership

- **DataGain's** proprietary information stored on electronic and computing devices whether owned or leased by **DataGain**, the employee or a third party, remains the sole property of **DataGain**. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of **DataGain** proprietary information.
- Users may access, use or share **DataGain** proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within **DataGain** may monitor equipment, systems, and network traffic at any time, per CISO's Audit Policy.
- **DataGain** reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.2 Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the Remote Working Policy.
- System level and user level passwords must comply with the Password Protection Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from a **DataGain** email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of **DataGain**, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

2.3 Laptop/Desktop System Usage

- The company provides laptop to the users once they complete their training period. No critical data access has been provided to the users in the training period. The training period consists of 1 month to 6 months based on the role. The company issues laptop after taking the approval from the immediate reporting manager.
- Company laptops are not issued to "Data Analyst" users as they do not have access to download/upload any sensitive information. Company has issued laptops to a few tenured Data Analyst users as approved by their reporting manager. Exceptional cases are handled separately.
- Users are responsible for protecting the confidentiality/availability/integrity of their systems data.
- The assigned user of the system has to maintain full responsibility of the security of the system issued to him/her.
- Users are requested not to remove the Licensing sticker attached to the assets.
- Self-servicing of laptop/desktop and changes to hardware/software configuration without IT department approval is strictly prohibited.
- Users will bear the servicing cost of physical damages done to the company Assets. The Company does not charge for regular wear and tear of assets but does expect the employee to handle company assets with care such that the life of asset is prolonged. Any wear and tear beyond the normal expected rate will be charged to the employee as such.
- Users can mention necessary specifications needed for their job function before taking handover from the IT Department.
- Only legally valid and business-related applications software to be installed. No un-licensed software or applications may be used in the organization.
- Employees may not take the notebook computer for repair to any external agency or vendor at any point of time.
- Any software bought from outside vendors or contractors should be installed only after proper permission from the IT Department has been obtained.
- All business files should be stored in the central file server in their respective departments' folders. Access will be provided only based on NEED TO KNOW principle.
- Critical information with classification CONFIDENTIAL or RESTRICTED should be stored in local laptop/desktop after management approval and should be strictly password protected. All such data / files should also be backed up to secured zone on file server.
- If any system is used by multiple users, no sensitive information should be stored in it.
- Systems assigned to third parties or contractors should not have any sensitive information stored in it.
- Using Laptop/Desktop without installation of company-approved Antivirus client software

is strictly prohibited.

- Using Laptop/Desktop without domain controller authentication is strictly prohibited.
- Laptop/Desktop should always be in locked condition when not in use. Users will ensure the Laptop/Desktop is protected from unauthorized usage and access to information.
- The admin password is required to install any software on the **DataGain** systems, no user can install or uninstall a software on their system without admin password. The admin access at **DataGain** remains with only the selected authorized personnel.

2.3.1 Fault Logging

- Any laptop given to the IT department for repair, for such laptops, the ownership of the security shall lie with the IT department till the laptop is handed back to the user.
- In the case of theft/missing of laptops, the incident is to be reported to the IT department immediately and users shall agree to the necessary corrective actions taken.
- All the system faults should be logged through email or verbal and rectified in a systematic manner and records should be maintained for the same.

2.4 Management Rights to Review

- The Management reserves the rights to, without prior notice, examine e-mail, personal file folders, Web browser Book Marks, Cache files etc. to ensure adoption to **DataGain** Policies or Procedure as per legal requirements.
- All the e-mails are **DataGain** property and are liable to be read, intercepted and if necessary, deleted.
- **DataGain** may also disclose e-mail messages sent or received to law enforcement officials without prior notice to the employees who may have sent or received such messages. Users should restrict their communications to business matters in recognition of this electronic monitoring.
- The Management must, however, explicitly authorize monitoring of e-mail for the above-mentioned reasons. Unless specifically delegated, the task of monitoring e-mail messages by all other employees is prohibited. **DataGain** should ensure backup of e-mail messages stored in the server, as per the backup guidelines.

2.5 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

- Under no circumstances is an employee of **DataGain** authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing **DataGain**-owned resources.

2.5.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- 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 **DataGain**.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which **DataGain** or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting **DataGain** business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- 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.
- Using a **DataGain** computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any **DataGain** account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to CISO is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the **DataGain** network.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- 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.
- Providing information about, or lists of, **DataGain** employees to parties outside **DataGain**.

2.5.2 Email and Communication Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within **DataGain's** networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by **DataGain** or connected via **DataGain's** network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.5.3 Blogging and Social Media

- Blogging by employees, whether using **DataGain's** property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of **DataGain's** systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate **DataGain's** policy, is not detrimental to **DataGain's** best interests, and does not interfere with an employee's regular work duties. Blogging from **DataGain's** systems is also subject to monitoring.
- **DataGain's** Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any **DataGain** confidential or proprietary information, trade secrets or any other material covered by **DataGain's** Confidential Information policy when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of **DataGain** and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when

blogging or otherwise engaging in any conduct prohibited by **DataGain's** Non-Discrimination and Anti-Harassment policy.

- Employees may also not attribute personal statements, opinions or beliefs to **DataGain** when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of **DataGain**. Employees assume any and all risk associated withblogging.

3 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the policy owner.

4 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.