

Granicus

ACCEPTABLE USE POLICY

August 16, 2024 Version 2.3

T A B L E O F C O N T E N T S

1	INTRODUCTION.....	3
1.1	Purpose.....	3
1.2	Background.....	3
2	SCOPE.....	3
2.1	Users.....	3
2.2	Systems.....	3
3	ENVIRONMENT.....	3
4	STEWARDSHIP.....	4
5	COMPLIANCE.....	4
6	SOCIAL NETWORKING USE.....	6
7	RECOURSE.....	6
8	OWNERSHIP AND REVIEW.....	7
8.1	Contact Information.....	7

1. Introduction

1.1 PURPOSE

The purpose of the Granicus Acceptable Use Policy is to ensure the protection of Granicus' Customers, Partners, and Employees from illegal or damaging actions by individuals, either knowingly or unknowingly. This policy outlines the acceptable use and required level of security of computing resources used to access, store, process, and/or transmit Granicus information resources.

This policy also provides management support for proper conduct principles, and unambiguously demonstrates to stakeholders the management commitment to a healthy and productive environment. This policy is both approved and supported by the Granicus Vice President of Human Resources.

1.2 BACKGROUND

Granicus, including its subsidiaries, intends to make information resources available to employees and authorized users with the expectation that these resources will support a valid business use. Each resource introduces inherent risks. In response to those risks Granicus creates and maintains this Acceptable Use Policy governing the usage of Granicus information resources.

The acceptable use of corporate resources requires sensitivity to the Granicus environment, responsible stewardship of assets that the stakeholders have entrusted to Granicus, and compliance with all Legal and Ethical responsibilities.

2. Scope

2.1 USERS

This policy applied to Granicus Employees, Contractors, Consultants, and Temporary Workers (e.g.s, interns) granted access to Granicus' information resources, such as devices, networks, and information.

This policy will affect all users of Granicus information resources.

3. Environment

Objective: *To establish an environment to optimize the Granicus mission.*

- A. All entities granted access to Granicus information assets shall be required to complete a non-disclosure agreement (NDA) to uphold information confidentiality. Failure to complete the agreement shall result in denial of access.
- B. The ability to access information or content, whether internal or external, does not imply any consent regarding the use of such assets.
- C. The act of downloading/uploading, creating and/or displaying items of a pornographic or prurient sexual nature creates an uncomfortable or hostile environment, and such activity is prohibited.
- D. The act of downloading /uploading, creating and/or displaying items of a racist or sexist nature, or negatively targeting any identifiable group, can create an uncomfortable or hostile environment and such

activity is prohibited.

- E. The act of downloading /uploading, creating and/or displaying items that elicit an uncomfortable response, or are deemed inappropriate, is prohibited. Management reserves the right to determine what is or is not appropriate.
- F. There is no guarantee of privacy while using Granicus infrastructure. Information created or stored on Granicus equipment is considered the intellectual property of Granicus. Management reserves the right to monitor workstation activity, run security assessments and examine incidents on any equipment at any time. Employees can refer to the Granicus Employee Privacy Policy in Confluence for more details regarding their privacy rights.

4. Stewardship

Objective: *Retain stakeholder trust by demonstrating responsible stewardship toward corporate assets.*

- A. Downloading of large or streaming files requires excessive bandwidth. To ensure availability of Granicus information resources for all business needs, all high bandwidth applications shall be justified by business requirements.
- B. Attempts to intentionally damage or hinder Granicus information resources, such as tampering or reverse engineering or the introduction of viruses, worms, or other forms of malicious software is prohibited.
- C. Uncontrolled software often harbors malicious intent and may result in the inadvertent introduction of viruses, worms, Trojans, and other forms of malicious code that can pose risks to the confidentiality, integrity, and availability of our systems. Intentionally introducing any software not approved by the Information Security Program is prohibited. All software, tools, and external resources should only be used once properly vetted, reviewed, approved, obtained and implemented via prescribed methods and channels. All software used in conducting business and providing solutions should come from trusted sources to prevent the introduction of malicious code or vulnerabilities into our environments and infrastructure.
- D. Individuals, in the course of their tenure with Granicus may be exposed to protected information and are bound by the requirements of the [Granicus Information Classification and Handling Standard](#). Protection requirements specifically address the protection of removable storage media such as CD-ROM.
- E. Individuals, in the course of their tenure with Granicus may be issued mobile computing devices such as laptop computers and are therefore bound by the requirements of the Granicus Information Classification and Handling Standard and any other Standards applicable to the use of mobile devices. Protection requirements specifically address the concerns of sensitive data resident on portable computing devices at home, in automobiles, or other areas with marginally controlled physical security.
- F. Usage of Granicus information resources shall be based upon business requirements. Frivolous usage is prohibited.
- G. Information Security is everybody's responsibility, and it is every individual user's responsibility to report to Help Desk any real or suspected violation of Granicus policies and/or standards.
- H. Personal Data. Employees should use personal data only for the purpose that are relevant and compatible with the purpose for which it was collected. Employees can refer to the [Privacy Policies](#) in Confluence for more detail on purpose of processing. Additionally, personal data received in connection with individual rights request under privacy regulations (such as General Data Protection Regulation or California Consumer Privacy Act) should only be used to verify the validity of the request

and/or to respond to the request.

5. Compliance

Objective: *To comply with all legal and ethical responsibilities*

- A. Unauthorized reproduction of copyrighted works, such as software and documentation, is an infringement of intellectual property laws, and is prohibited. Unauthorized duplication of copyrighted material may subject users and/or the Company to both civil and criminal penalties under the United States Copyright Act.
- B. Employees may not duplicate any licenses, software or related documentation for use either on the Company's premises or elsewhere unless such duplication is expressly authorized by the licensing agreement with the publisher.
- C. Employees must not provide licensed software to any outsiders including contractors, customers, or others. Workstations shall be cleared of sensitive information and locked while unattended, and set a password on automatic screen savers.
- D. Desks and work surfaces shall be cleared of sensitive information while unattended and at the end of the work shift prior to leaving.
- E. Printers and other devices which could disclose sensitive information in printed form shall be cleared of such information in a timely manner.
- F. Use of Granicus communication media, such as email and instant messaging, to send threatening or harassing communications is prohibited, and may result in investigation by relevant law enforcement authorities.
- G. Certain employee or customer records, such as Social Security numbers, are protected against unauthorized access. Disclosure, either accidental or intentional, may subject the responsible party to the full measure of recourse.
- H. Any attempt to circumvent access controls, or "hacking", unless it is done by a role that is authorized to conduct these types of activities for a specific business purpose, is a violation of the federal Computer Fraud and Abuse Act, as well as state and local law, and may subject the violator to prosecution.
- I. Utilization of Granicus information resources for personal gain, such as gambling or self-marketing, is unethical and hence prohibited.
- J. Casual and limited personal use of Granicus information resources is allowed on a non-interfering basis. Sending and receiving an occasional personal email, and "break time" web surfing may be considered examples of casual personal use.
- K. Sharing user accounts and passwords hinders the ability to hold users accountable for their activities and may result in false accusations against the legitimate account holder. Account sharing may also result in identity theft. Sharing of accounts, passwords and other user access information is strictly prohibited.
- L. Use of Passwords. Passwords for all systems will be at least 12 characters and complex, including all of the following: upper and lower case letters, numbers, and special characters. Passwords must be unique and not shared by users.
- M. Information spill. If you see information you're not authorized to access, you are prohibited from disseminating, distributing or copying the information. You are required to report this Information Spill to the Information Security Department.
- N. Mobile devices. In the event that you lose a mobile device you need to report this immediately to helpdesk so they may remote wipe the device to remove Granicus information.
- O. Granicus Data. Client data contained within a Granicus database must not be moved, copied, or otherwise transferred to an individual IT resource or lower environment for purposes of research, software

development, testing, training or other activities.

- P. Email Encryption. Email containing confidential data must be encrypted before sending externally and password should be sent via a different method from the data. Example- Email the encrypted file and text the password.
- Q. Former Employees. Former employees are not permitted into the office without an approved business purpose.
- R. After Hours. Employees hosting after-hours, business-related events must complete the "Off Hours" form, receive approval, and comply with all policies in the form.
- S. Travel. Employees are not permitted to take their standard work-issued laptop to areas of significant risk as determined by the United State Department's "Travel Advisory" (Level 3 and Level 4). If an employee has to travel to a location of significant risk, a "travel" laptop with standard base configuration will be issued.

6. Social networking use

Objective: *To limit business risk exposure related to the use of social networking*

- A. Social networking posts must conform to all relevant requirements of both this policy and the Information Security Program.
- B. Employees shall not claim to represent Granicus in social network postings or messages unless specifically authorized to do so by management.
- C. Do not, under any circumstances, defame or otherwise discredit the products or services of the Company, their partners, affiliates, customers, vendors, or competitors.
- D. Postings shall not use Granicus's logo, trademark, proprietary graphics or photographs of the Company's premises, personnel or products without explicit management approval.
- E. Postings, whether business-related or personal, must not contain information that Granicus considers derogatory or damaging to the company's reputation and goodwill. Any such posts, even those made anonymously, are subject to investigation and appropriate remedial action by the Company.
- F. Violations of the above rules may result in both disciplinary action (recourse) and remedies in law.

Note: Immediately notify the Human Resources Department whenever there is a change in your role, assignment, or employment status and/or when access to the system is no longer required.

7. Recourse

Objective: *To ensure management of policy violations*

Compliance with this Acceptable Use Policy is a condition of resource usage as well as a means for enforcement. Users shall have no expectation of privacy while using Granicus information resources. Granicus reserves the right to monitor usage of Granicus information resources and to take relevant disciplinary action based upon inappropriate use. Recourse is managed by the Granicus Human Resources Department.


8. Ownership and Review


This Policy is owned by the Human Resources Chief Human Resource Officer. This Policy shall be reviewed on a yearly basis. Change to this document shall be in accordance with the ISMS Document Control standard. The Chief Information Security Officer (CISO) is responsible for approving this policy at least annually.

8.1 CONTACT INFORMATION

Carrie Cisek, Chief Human Resource Officer

E  carrie.cisek@granicus.com

T  651-757-4114

L  408 St. Peter St., Suite 600, St. Paul, MN, 55102