Catalyst Campus for Technology & Innovation (CCTI)

IT Acceptable Use Policy

26 September 2021

Approval			
Name	**Department**	**Role/Position**	**Date approved**
Justin Kirk	IT	IT Director	04/24/2022
			MM/DD/YYYY

1 Overview

The purpose of this policy is to establish acceptable and unacceptable use of physical space, data, computing, and network resources at **Catalyst Campus for Technology & Innovation (CCTI) ("company")** in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

2 Scope

"Personnel" is defined as all employees, contractors, consultants, temporary, and other workers at the company. Personnel must adhere to this policy. This policy applies to all company data, computing, networks, physical facilities, and any other information asset that connects to the company's network. This policy also applies to any personnel physically located at the company's site, even if that person possesses no computing asset. Personnel may submit an exception request for consideration to the IT Helpdesk.

"Proprietary" is defined as any company information not marked for public release, any company's customer information not marked for public release, or any Government Controlled Unclassified Information (CUI). The CUI program replaces existing approaches such as For Official Use Only (FOUO), Sensitive but Unclassified (SBU), and Official Use Only (OUO); however, "CUI" is not the standard labeling convention, so terms such as "FOUO" continue.

3 Policy Statement

Use of company data, networks, computing, or physical facilities for personal use is not authorized. The computing resources and facilities are the property of the company and shall be used for legitimate activity related to company business which may also include computer-based learning, certification training, and higher education.

The company provides computer devices, networks, and other electronic information systems to meet mission goals and must manage them responsibly to maintain the confidentiality, integrity, and availability of its assets. Personnel are responsible for exercising good judgment regarding appropriate use of company resources.

3.1 Privacy

Human Resources (HR) and Finance maintain and protect personally identifiable information (PII). PII, such as a social security number that can identify an individual, is protected within the company. Non-authorized personnel should not store, transmit, or process PII. PII is for company business use and is not allowed for personal use on company assets.

For security, compliance, and maintenance purposes, authorized IT and cybersecurity personnel may monitor and audit equipment, systems, and network traffic per Section 3.8, System Auditing and Security Testing. As part of that, personal privacy using company assets should not be assumed:

3.1.1 *Company corporate and guest networks.* The company monitors all connections, uniform resource locator (URL) access, and correlates data for cybersecurity posturing. There should be no expectation of personal privacy when using a company corporate or guest network.

3.1.2 *Company computing.* All laptops, servers, virtual machines, cloud computing, and networking equipment are monitored to the application level. The company will attempt to notify personnel if remote access is required; however, permission is not required. There should be no expectation of personal privacy when using company computing.

3.1.3 *Non-company computing.* Any networking device on the corporate or guest network is subject to section 3.1.1. An example device may be a personal phone allowed to connect on the guest network. Some personnel are allowed additional privileges for their device under the Mobile Device policy to access functions such as e-mail. There should be no expectation of personal privacy.

3.1.4 *Security Cameras.* The company may use cameras to monitor and record video, where allowed by contract and law. Example locations include building exterior, entrances, hallways, stairways, laboratories, and server rooms. There should be no expectation of personal privacy where video recording is allowed by law.

3.2 Physical Security

3.2.1 Print jobs should be removed from printers immediately after printing.

3.2.2 Physical copies of proprietary data shall be protected and not visible when personnel are away from their work area:

3.2.2.1 If the personnel's office or cubicle is locked, maintain in a drawer

3.2.2.2 If the personnel's office or cubicle does not lock, then maintain in a locked drawer

3.2.3 Company locations may employ the use of proximity badge access. Proximity badges may be used to secure a building, suite, or specific areas requiring access control (e.g., sever room). Proximity badge use is intended for the authorized owner only. Logs of badge use are maintained and may be audited per Section 3.8 System Auditing.

3.2.4 Where a company facility does not employ proximity badges, company

personnel are responsible for ensuring access to the facility is controlled. Opening/closing procedures are recommended to ensure the facility security is properly maintained. Cipher codes or keys are issued by authorized personnel only.

3.2.5 Doors that are intended for security should be closed. Doors that are propped open for events such as moving shall be monitored by personnel. If personnel identify a security door that is propped open, they should secure the door and notify the Facility Security Officer (FSO).

3.3 Information Assets

3.3.1 Personnel are responsible for the security of data, accounts, and systems under their control.

3.3.2 Personnel must follow the company Password Policy. If there is any conflict, the Password Policy takes precedent over this section. At a high-level, the Password Policy content is that passwords must be complex and 14 characters long; passwords may not be reused (domain and online); passwords must be kept secure and not shared with anyone (colleague or personal); passwords (such as Wi-Fi) may not be written on whiteboards; and desks must be clean of written passwords unless securely locked.

3.3.3 You must ensure through administrative, legal or technical means that proprietary information always remains within the control of the company.

3.3.4 Conducting company business that results in the storage of company information on personal or non-company-controlled environments, including devices maintained by a third-party with whom the company does not have a contractual agreement is prohibited.

3.3.4.1 This specifically prohibits the use of an e-mail account that is not provided by the company or its customer and partners for company business.

3.3.4.2 A non-exhaustive list of unauthorized third-party storage: Google Docs; Google Drive, Amazon Drive, Box, Dropbox, Hightail, and MediaFire.

3.4 Computing Assets

3.4.1 Personnel are responsible for ensuring the protection of assigned company assets. Computing assets are considered secured while in a company facility that is secured by cipher, key, or fob access. Laptops left at the company overnight that do not have access control implemented should be placed in a locked drawer or cabinet. Promptly report any theft of company assets to IT or HR.

3.4.2 All company-provided devices (Androids, iPhones, iPads, laptops, and workstations) must be secured with a password-protected screensaver with

the automatic activation feature set to 10 minutes or less.

3.4.3 Personnel must immediately lock the screen or log off when the device is left unattended.

3.4.4 Personnel shall not interfere with corporate device management or security system software, including, but not limited to anti-virus, remote management, and asset tracking tools installed by IT.

3.4.5 Modifying registry settings or changing DNS is strictly prohibited.

3.4.6 Company to company remote desktop to laptops is not enabled by default. It is allowed on a case-by-case basis by coordinating with IT.

3.4.7 Remote access from a personal device to company assets is not permitted. This includes remote desktop (using native operating system tools or any third-party applications); Virtual Private Network (VPN); and document and source code repositories.

3.4.8 Personal removable media storage of any type is not allowed in any form or function within the company's environment. Personal storage devices shall not be used for storage of any company information or be used with company hardware.

3.4.9 Company owned removable media storage containing any proprietary data must be maintained under positive control (in possession or physically locked) and erased after transfer, or the removable media must be encrypted using the minimum password standard.

3.4.10 When personnel receive a reboot popup from the IT remote management software, the system must be rebooted within one week. After a week is exceeded, IT will force reboot the computer as part of the patching process. Personnel may or may not be notified of this forced reboot ahead of time. NOTE: A shutdown and start are not the same action as a reboot which forces patching.

3.5 Network Use

Personnel are responsible for the security and appropriate use of company network resources under their control. Using company resources or any company network type for the following is strictly prohibited:

3.5.1 Causing a security breach to the company or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic except as authorized for the purposes of debugging Braxton developed software.

3.5.2 Review or distribution of any adult content.

3.5.3 Unauthorized viewing or use of another person’s computer files, programs, or data is prohibited.

3.5.4 Causing a disruption of service to the company or other network resources, including, but not limited to ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.5.5 Introducing any type of access point (Bluetooth, wireless, switch, router, etc.), honeypots, honeynets, or similar technology. Approved personnel following a change management process of their program may modify laboratory networks.

3.5.6 Violating copyright law, including, but not limited to illegally duplicating or transmitting copyrighted pictures, music, video, and software.

3.5.7 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

3.5.8 Intentionally introducing malicious code, including, but not limited to viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

3.5.9 Port scanning or security scanning unless authorized in advance by the IT Lead.

3.5.10 Written permission and proper procedures must be followed in the event of computer reassignment and or transfer of licenses.

3.6 Electronic Communications

Using company resources for the following are strictly prohibited:

3.6.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates company policies against harassment or the safeguarding of proprietary information.

3.6.2 Sending spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

3.6.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

3.6.4 Posting the same or similar non-business-related messages to large numbers of forums, newsgroups, or social media.

3.6.5 Exceeding authority in representing the opinion of the company.

3.7 Software Usage

The company purchases and licenses software or applications from a variety of sources. Any duplication of software or application except as permitted by related license agreements is a violation. Installing unauthorized software or applications on a computer system, workstation, or network server within the company can lead to potential system failures, system degradation or viruses.

3.7.1 Authorized applications and software

3.7.1.1 Only software on the "authorized applications and software" list may be installed by IT. To limit policy length and ease of software list updates, the separate "IT-Policy-Acceptable Use Addendum A – Authorized Applications" contains the "authorized applications and software."

3.7.1.2 As a rule, do not install anything unless coordinated through IT.

3.7.1.3 To request software additions to the acceptable use addendum, open an IT trouble ticket.

3.7.2 Some personnel outside of the IT department possess administrator credentials through the "Administrator Account Access Process" with signed paperwork on file. If there is any doubt of what is authorized, any person with administrator access should coordinate software installation through IT.

3.7.3 Licenses may not be uninstalled from one user's machine and re-installed on another user's machine without written permission.

3.8 System Auditing and Security Testing

The purpose of this section is to advise users of security scanning procedures and precautions used by the company to audit the network and systems. Security testing on all company networks requires the prior approval of the IT Lead. All personnel or entities, unless authorized, are prohibited from performing any such audits.

3.8.1 Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents to ensure conformance to the company's Information Technology and Information Systems Security policies
- Monitor user or system activity where appropriate
- Monitor physical access to company facilities where appropriate

3.8.2 Audits may be conducted against:

- Any company asset
- Any device on the corporate network (wired, and if applicable, wireless)
- Any wireless device, personal or corporate, connected on the guest network
- Any device connected through the company's VPN
- Any device used as a Personal Electronic Device (PED) and according to that policy

3.8.3 Audits may include:

- User and/or system level access to any computing or communications device
- Access to information that may be produced, transmitted or stored on company equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on company networks
- Penetration testing

- Password auditing
- Security auditing
- Security review
- Scanning for Personally Identifiable Information (outside of authorized areas declared by HR and Finance)

3.8.4 Software shall not be duplicated, reproduced, or installed on more than one machine without prior written authorization.

4 Reporting & Support

4.1.1 **Emergency. Call 911**

4.1.2 **Cybersecurity Event.**

Personnel shall conduct the following:

4.1.2.1 Disconnect wired and wireless networking. Leave the machine on.

4.1.2.2 Notify IT. IT will then use the internal Incident Response Plan to follow assessment as well as remediation and reporting steps if necessary.

4.1.2.3 Do not discuss the details of the event externally to the incident response people assigned to the event. The company will appoint a person to manage all communication.

5 Travel Considerations

5.1.1 Whenever proprietary information is carried by personnel into a foreign country, the information must either be stored in some inaccessible form, such as an encrypted external storage media, or must always remain in physical possession.

5.1.2 Personnel will not take Secret Government information into another country unless permission is coordinated with the FSO.

5.1.3 Personnel in the possession of mobile devices (laptop, notebook, palmtop, smart phones, personal digital assistants, or any other device) containing proprietary information shall not check these computers into the airline luggage systems. These computers must remain in physical possession of personnel as hand luggage.

5.1.4 All personnel returning from travel out of country must have their company devices inspected by the IT department before connecting to the company network. This inspection is required to check for malicious software or other security vulnerabilities introduced during travel.

6 Video and Still Camera Features

6.1.1 Personnel shall not use the video or still camera features on any mobile device, including smartphones and tablet computers to capture images that may depict proprietary company information, including but not limited to customers, documents, computer displays and output.

6.1.2 Employees and partners must not use the video or still camera features on any mobile device, including smartphones and tablet computers to capture images within any company secure area, including but not limited to areas where proprietary procedures are performed, proprietary devices or equipment are used, or non-public information is processed, stored, or transmitted.

7 Enforcement

The company reserves the right to monitor and record the usage of all facilities and equipment, and all software which is the property of the company by ownership, lease, rent, sponsorship or subsidy. If the company has reason to believe that activities are taking place that are contrary to this policy or state or federal law or regulation, the company has the right to use information gained in this way in disciplinary, civil, or criminal proceedings. Additionally, personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. An individual's access to computer resources may be suspended immediately upon the discovery of a violation of this policy.

The company follows NISPOM regulations, and **the company will notify the FBI if espionage, sabotage, terrorism, or subversive activities are suspected.**

8 External References

- IT-Policy-Acceptable Use - Addendum A - Authorized Applications
  - This addendum lists company allowed software and a non-comprehensive list of unallowed software.
- IT-Policy-Password Policy.
  - The password policy is summarized in this policy. The full password policy expands concepts and provides more detail.

9 Revision History

Date of Change	Version	Responsible	Summary of Change
2/23/2020	1.0	Jim Robinson	Policy Creation
9/26/2021	1.1	Justin Kirk	Clarification, minor updates
4/24/2022	1.2	Justin Kirk	Update Policy

10 IT Acceptable Use Policy Acknowledgement

Acknowledgement may be through initial in-processing or sent to the Human Resources (HR) department.

- I have read and agree to the terms of the IT Acceptable Use Policy
- I understand that there is no expectation of privacy while using company computing or networks

_____	_____	_____
*Printed Name	*Signature	*Date

*Fill out the mandatory fields and provide a copy to HR for approval.