IT Acceptable Use Policy

Metergy Solutions Inc.

Effective as of December 1, 2020.

™Metergy Solutions and the design are trademarks of Metergy Solutions Inc.

Table of Contents

1. Policy Statement

All of the defined terms set out in this Policy shall have the meaning as set out in Appendix A unless the context dictates otherwise.

This Policy describes appropriate uses of the Metergy Network and IT Assets for the purpose of protecting against inappropriate use that may compromise the Metergy Network or IT Assets and expose Metergy to excess risk, reputational damage or non-conformance to laws or regulations.

The Policy expands on the Code and is intended to be read in conjunction with Metergy's IT Security Policy.

This Policy applies to Metergy and its subsidiaries and affiliates. Metergy's systems and information are to be used for the sole benefit of Metergy by Users in the course of fulfilling their assigned duties and responsibilities. Users must only access or retrieve stored information as authorized or required in the course of their employment or contract and in accordance with Metergy's IT Security Policy. While incidental personal use of IT Assets (including Mobile Devices) is permitted, it must not adversely affect the operations, security, or reputation of Metergy. Explicitly prohibited are using IT Assets for personal gain, degrading quality of services, circumventing security policies or processes, or bypassing monitoring and enforcement technologies.

All Users have a responsibility to protect the IT Assets and Information.

To ensure that the use of the Metergy Network and IT Assets are consistent with the Code, the IT Security Policy and Metergy's other policies, Metergy may monitor the use of the IT Assets including reviewing information and messages on the Metergy Network and maintaining recordings of such use. Users do not have any right to prohibit access by Metergy to any message or information placed in or transmitted by the Metergy Network or IT Asset.

Compliance with this policy is mandatory for all Users.

2. Scope

This Policy applies to all Users.

3. Roles, General Responsibilities

Executive management is responsible for ensuring balanced policies are developed, procedures to identify risks are in place, programs are established to mitigate risks, and that security management remains adequately funded. Executive management will ensure that policies align to Applicable Laws such as *Canadian Anti-Spam Legislation (CASL)* and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

Line of Business Managers are responsible for ensuring that the requirements of this Policy are implemented and supported within their business units, ensuring their emteam members acknowledge an understanding of this Policy and related standards, procedures, and guidelines.

Users are responsible for acknowledging and complying with this Policy and related standards, procedures, and guidelines, as well as the Code. Team members are required to support compliance assessments and investigations as necessary, including any enforcement procedures.

4. User Obligations

4.1. By using an IT Asset, the User acknowledges and agrees to the terms and conditions of this Policy. The User further acknowledges and agrees that any infraction of this Policy may result in disciplinary action, up to and including termination of employment or contractual relations, as applicable.

4.2. Users acknowledge and agree that the Metergy Network and IT Assets are to be used responsibly, ethically and lawfully for Metergy business purposes.

4.3. Users acknowledge and agree that while Metergy desires to provide a reasonable level of privacy for the User, the Information created, received, stored, or deleted by the User on the Metergy Network or IT Asset is the property of Metergy and may be accessed by Metergy at any time with or without notice.

4.4. Users will exercise good judgment in regards to the reasonableness of personal use of the Metergy Network and IT Assets. In particular, Users will limit personal use of Mobile Devices issued by Metergy. If Users have uncertainty concerning the reasonableness of personal use of the Metergy Network and IT Assets, the User should consult their Manager or IT. See section 7 (General Device Usage) and section 8 (Mobile Device Usage) for details on usage and charge backs related to personal use.

4.5. Users are prohibited from using any Non-Metergy IT Asset for Metergy business purposes, such as accessing the internal Metergy Network and storing information.

4.6. Users will avoid actions that could potentially degrade performance of the Metergy network or disrupt Metergy business. These actions include, but are not limited to personal peer-to-peer file transferring, crypto mining, port or security scanning, pinged floods, or any other technologies that would lead at any time to a Denial-of-Service (DoS) on the Metergy Network.

4.7. Users will report any actual or potential breaches of this Policy immediately upon discovery of such actual or potential breach to IT, the User's Manager or to Human Resources, at the preference of the User based on the nature of the breach and related circumstances.

4.8. Users are strictly prohibited, with no exceptions, from using the Metergy Network and IT Assets to engage in any of the following activities, each of which constitutes a Security Incident:

a. Installing unauthorized hardware or software on an IT Asset or Metergy Network. For certainty, any hardware or software not installed by IT will be deemed unauthorized hardware or software with the exception of mobile applications on smartphones issued by Metergy. Downloading and installation of mobile applications on a smartphone are subject to the following criteria: 1) the downloading, installation and use of the application must be at no cost to Metergy, 2) the application must not interfere with work duties, 3) the application must not contravene this Policy or any other Metergy policy, 4) the application must not be transmitting or exposing any Metergy information to unauthorized individuals, systems, or entities. IT reserves the right to prohibit and remove any mobile application without notification. Users may also be asked to remove any application on the device that has the potential for creating liability of any kind for Metergy.

b. Disclosure of a User's Password to any other person or permitted use of the User's account by any other person, other than if provided to authorized IT personnel to facilitate management of IT Assets.

c. Sharing account information and passwords for any systems, either with other authorized Users or with contractors or individuals or groups not employed by or under contract to Metergy.

d. Attempts to access or actions intended to facilitate access to IT Assets for which the User is not authorized.

e. Circumvention of access controls to access the Metergy Network, Metergy accounts, or Metergy assets.

f. Communicating under disguised identification or impersonating another person, including another User.

g. Engaging in any form of harassment, such as making discriminatory, disparaging, defamatory, or sexual communications, whether through language, frequency or size of messages.

h. Using the Metergy Network or an IT Asset to access or transmit material that may be interpreted as discrimination, sexual harassment, or creating a negative work environment or is otherwise in violation of the Code or any other Metergy policy.

i. Circumventing any measures taken by Metergy to prohibit access to certain websites and applications.

j. The access of, retention of or propagation of material that is offensive, obscene or indecent, including the deliberate viewing, transmitting, and/or printing of pornographic images.

k. Engaging in personal use that is unlawful, unprofessional, irresponsible and/or detrimental to Metergy's best interests, interferes with the User's regular work duties or otherwise violates the Code or any other Metergy policy.

l. Executing any form of Metergy Network monitoring intended to intercept Information not intended for the User, unless such activity is permitted within the scope of the User's employment duties, as authorized by the SVP IT or delegate.

m. Infringement of intellectual property rights of Metergy or any third party, such as copyright, trade-mark, patent, designs or the installation or distribution of "pirated" or other software products that are not licensed for use by Metergy.

n. Sending non-business related messages to large numbers of Users or non-Users, within or outside the Metergy Network; for example, spam.

o. Any activity that compromises the confidentiality, integrity, or availability of Information.

p. Any activity that creates any legal or contractual obligation(s) on behalf of Metergy, unless expressly authorized by Metergy.

q. Actions or inactions which intentionally or unintentionally aid the distribution of any malicious program into the network or system (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).

r. Posting of defamatory comments about Metergy, its shareholders, directors, management, contractors, or team members on social networking sites, blogs, forums, or any other network resources.

s. Transmission or copying of Information onto Portable Storage Media without encryption enabled, as prescribed.

t. Transmission of Information to data repositories not explicitly under contract to Metergy for data retention or data hosting services, including file offsite storage services, online storage services, and external e-mail accounts.

u. Any action, inaction or activity whose purpose is to indirectly effect a prohibited activity listed above.

5. IT Obligations

5.1. IT will monitor User activity on the Metergy Network and IT Assets for the following purposes:

- To maintain security and operation of the Metergy Network, in accordance with the IT Security Policy.

- To monitor improper, unauthorized or excessive personal use, including any activity that would comprise a Security Incident.
- To enforce this Policy.
- To facilitate repayment from a User or charge-back to the User's department for excessive personal or inappropriate business use.
- To establish maximum usage limits appropriate for business use.
- To determine the appropriate devices for business use.

5.2. IT will block access to selected non-business internet sites in its sole and exclusive discretion.

5.3. IT will investigate and respond to all complaints or purported breaches of this Policy and will report such investigations to the President and other applicable Metergy Executives.

6. Software Acquisition and License Usage

6.1. Except as otherwise described herein, only software authorized and approved by Metergy is to be used in IT Assets. All software used must be properly licensed and approved. Compliance with license agreements will be enforced by Metergy.

6.2. Licensed software will only be copied in accordance with licensing agreements.

6.3. Unauthorized or illegal use of copyrighted software could result in corrective action, up to and including termination and/or criminal action.

7. General Device Usage

7.1. Security Measures: Metergy will adopt information security measures that may limit IT Asset functionality from time to time, such as screen lock time-out periods, password failures, and device encryption.

7.2. Personal Usage: All IT Assets are intended primarily for business use. Personal use is allowed, within reason, and compliance to all Metergy policies is expected, even if the device is being connected to non-Metergy networks. Personal use does not extend to family members' or friends' usage of IT Assets.

7.3. Physical Security / Loss, Theft or Compromise: The physical security of the IT Asset must be ensured at all times. If an IT Asset is lost, stolen or is damaged to the point it cannot function, or if it is believed to have been compromised in some way, the incident must be reported immediately. The User must contact the IT Service Desk as well as the User's Manager. The User must also fill out a Lost, Theft, Damage (LTD) form. In all cases, any associated cost will be charged to the User's department. The expense must be approved by the supervisor of the User's Manager unless the User or the User's Manager is a member of executive management.

7.4. Private Commercial Use: IT Assets must not be used for private commercial purposes except where the work is authorized by Metergy and is conducted in accordance with Metergy's policies.

7.5. Remote Access: When a User is not on Metergy's premises, VPN may automatically be connected and device activity may be monitored.

7.6. Portable Storage Media: Users can only use Metergy Portable Storage Media, such as USB, CD, or memory cards, on Metergy assets. Sensitive information should be storedon Portable Storage Media only when required in the performance of Users' assigned duties.

8. Mobile Device Usage

8.1. Mobile Devices are intended primarily for business use. However, personal use is allowed, within reason, and care must be taken not to incur additional charges. Information must be protected and segmented at all times from the User's personal data stored on the Mobile Device. Metergy reserves the right to wipe, disable or decommission the Mobile Device without prior notice. It is the User's sole responsibility to manage their personal data.

- Maximum acceptable usage for Mobile Devices will be established by the IT Department from time-to-time and posted on the Metergy intranet. Charge backs to recover personal use may occur above the current maximum usage levels as set by the IT Department.
- Metergy is not responsible for any cost or loss incurred through or as a result of the personal use of IT Assets.
- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system.

8.2. Mobile Devices should only be connected to a computer or other electronic device which has up to date anti-malware protection that complies with corporate policy.

8.3. Long distance calls not covered by the Users' Mobile Device plan or approved roaming package are not permitted unless they are business related. Anyone planning to travel outside of their home coverage area is required to submit a service request to the IT Service Desk at least one week in advance to request a roaming package which will reduce the roaming and long distance charges incurred.

- Failure to obtain a roaming package will result in a requirement to reimburse the company for any roaming charges incurred.
- The company may waive this requirement in its sole and absolute discretion.

8.4. The software and hardware configuration of each Mobile Device must be maintained. All required / defined corporate applications must be kept updated and in a functioning state. Users must not disable or subvert the security controls and configuration settings, including but not limited to:

- Removing, deactivating, and suspending any of Metergy’s applications installed on a Mobile Device including mobile device management (MDM) software deployed by Metergy.
- Disabling location services (GPS) in general, and specifically for corporate applications which require it to be active and on.

8.5. Metergy has the right to, at will:

- Monitor corporate messaging systems and data, including data residing on the User’s Mobile Device.
- Modify the registered Mobile Device configuration remotely, including wipe or reset to factory default.

9. Eligibility for Mobile Devices

9.1. Eligibility for a Mobile Device is based on the circumstances of the individual’s functional duties. A Mobile Device will only be provided by Metergy where it can be shown the Mobile Device is required to perform the duties of the job. Relevant criteria to assess eligibility for a Mobile Device include:

- The job responsibilities are such that the individual must be regularly available to respond via electronic communication and that access through secured internet is required when not on Metergy’s premises. The cost of the device or allowance offset can be supported by funding sources available to the department.
- The position requires the individual to be regularly on-call during off duty hours.

The application for a Mobile Device is to be made by the individual through the individual’s Manager and submitted to the IT Department. All requests must be submitted through the Metergy Service Desk, and sufficiently substantiate the need for the Mobile Device using the above criteria. All Mobile Device requests will be reviewed and approved by the IT End-User Services Manager.

9.2. Mobile Device types are limited to:

- Smartphones and mobile tablet devices
- The standard Mobile Device will change from time-to-time as determined by the IT Department

10. Email Usage

10.1. Users must use professional judgment when drafting and sending e-mails, recognizing Metergy records may be subject to disclosure pursuant to the *Freedom of Information* and *Protection of Privacy Act*.

10.2. Unsolicited advertising or spamming, or sending e-mails that purport to come from an individual other than the person actually sending the message is prohibited: for example, using a forged address.

10.3. Email content and signature line must, where possible, use the standard company signature line and adhere to corporate branding standards according to Email Signature Guidelines posted on the Metergy internal network. This also applies to Mobile Devices that have Metergy email accounts set up.

10.4. Users will include the standard corporate disclaimer at the end of all e-mails sent from the User's e-mail account.

10.5. Users are prohibited from using another User's e-mail account to either send or receive messages without written authorization from that team member.

10.6. Users must not manually or automatically forward electronic-mail containing Confidential Information to any e-mail address outside Metergy networks: for example, forwarding Metergy e-mail to unmanaged devices or accounts is prohibited except in exceptional circumstances. Users will promptly report such exceptions to IT, the User's Manager or to Human Resources, at the preference of the User based on the circumstances.

10.7. Metergy email accounts should be used primarily for Metergy business-related purposes; personal communication is permitted on a limited basis, but non-Metergy related commercial uses are prohibited.

10.8. Users are prohibited from using unauthorized third-party email systems and storage servers such as Google, Yahoo, and Outlook etc. to conduct Metergy business, to create or store any binding transactions, or to retain emails on behalf of Metergy. Such communications and transactions should be conducted through proper channels using Metergy-approved documentation.

10.9. If a User suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Metergy IT immediately.

10.10. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type from an Metergy email account is prohibited.

10.11. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. Any phishing and malicious email must be reported to the information security team.

10.12. Users will comply with Applicable Laws, including Canadian Anti-Spam Legislation (CASL) and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

10.13. Users must comply with the e-mail Requirements set out in Appendix B of this Policy.

11. Voicemail Usage

11.1. Voicemail systems utilized or administrated by Metergy (including Mobile Device voicemail) may not be used to send messages that are offensive, slanderous, unlawful, unprofessional, irresponsible, detrimental to Metergy's best interests or otherwise violate any Metergy policy.

12. Connectivity and Network Usage

12.1. Incidental personal use of the internet while working is permitted, including the use of social media sites, so long as the usage complies with Metergy's IT Security Policy*.* Downloading large amounts of data, such as from video or radio streaming sites, should be kept to a minimum as the Metergy Network could be affected for normal business uses. Depending on business needs, software restricting large downloads and streaming may be employed to constrain Users' usage of non-business related internet usage.

12.2. Remote connections to the Metergy Network via VPN's over the internet may be granted to Users on an as-needed basis in support of telework and other arrangements authorized by Metergy and its management.

12.3. Team members using IT Assets attached to the Metergy Network are prohibited from connecting to and/or accessing the internet through other sources (e.g., modem connection to alternate Internet Service Providers from or within the Metergy Network) without prior review and approval from the SVP IT or delegate.

12.4. While connected to VPN, all traffic destined for the internet must traverse the VPN and Users must not circumvent this measure for any reason.

12.5. Connectivity outside of Metergy's premises is preferred through VPN using an internet connection or secured wifi connection. In exceptional circumstances where connectivity is required and the above options are not available, a Mobile Device issued by Metergy can be used to establish connectivity.

- Maximum usage limits as determined by the IT Department are applicable in all circumstances.
- Rocket sticks will be decommissioned.
- Internet connections for home offices must be established directly between the User and their service provider. In the event that the User exceeds the usage threshold for legitimate business use on their home internet connection, as established by the IT department, the User may be entitled to reimbursement at the prescribed rate (posted on the intranet) for all or a portion of their home office internet connection through Metergy's expense reimbursement process, provided that the User's application is approved as set out below.
- The application for home internet reimbursement is to be made by the User through the User's Manager. All applications must be provided in written memo format with Director level approval, if applicable, and sufficiently substantiate and/or justify the

User’s need for business use of their home internet connection above the threshold established by the IT Department. The User’s Manager and Director must review and reapprove the User’s home internet reimbursement eligibility annually.

13. Personal Disclaimers

Personal opinions addressed to public groups, other companies or organizations on the internet through the Metergy Network must be pre-approved by the User’s Manager and must include the following disclaimer: “The views expressed here are mine and do not reflect the official position of Metergy Solutions Inc.”

14. Related Policies and Guidelines

14.1. IT Security Policy

14.2. Ransomware Payment Policy

14.3. Anti-Spam Policy

14.4. Code of Business Conduct

14.5. Discrimination and Harassment-Free Workplace Policy

14.6. Email Signature Guidelines

Appendix A: Definitions

Applicable Laws	All applicable laws, statutes, rules, by-laws, regulations, codes, treaties, ordinances, regulatory policies, including Privacy Laws, and all applicable directives, orders, judgments and decrees of or similar requirement made or issued by a governmental (including any regulatory or quasi-regulatory) authority having the force of law.
Code	Metergy's Code of Business Conduct.
Confidential Information	Proprietary, technical, business, marketing strategies, financial, trade secret, intellectual property, joint-venture, personal information about customers and team members that is not made available publicly.
DoS or Denial-of-Service	A denial-of-service (DoS) attack occurs when a targeted host or network is flooded with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. Services affected may include email, websites or other services that rely on the affected computer or network.
e-mail	An e-mail sent or received through a User's Metergy e-mail account.
Information	All data, documents and other materials electronically transmitted on the Metergy Network, including Confidential Information and intellectual property of Metergy.
IT	The Information Technology group, forming part of Metergy.
IT Asset	A telephone, computer of any kind (laptop, desktop, tablet, etc.), Mobile Device, external hard drive, USB key, compact disk, or any other electronic transmission hardware or software that is the property of Metergy.
IT Service Desk	Designated point of contact for all Users who require IT support. It is also known as the 'help desk'.
Metergy	Metergy Solutions Inc. and its subsidiaries and affiliates.
Metergy Executive	Metergy's President, Chief Financial Officer or Chief Legal Officer.
Metergy Network	The electronic communication system(s) used by Metergy to receive, collect, use, store, access, process, record, disclose, transfer, retain, destroy, manage or otherwise handle Information.
Mobile Device	An end-user orientated technological device designed to be moved freely and easily, which has the capability to allow Users to access the Metergy Network or Information including but not limited to smart phones (iPhone or Android), and tablet computers.

Non-Metergy Asset	A telephone, computer of any kind (laptop, desktop, tablet, etc.), Mobile Device, external hard drive, USB key, compact disk, or any other electronic transmission hardware or software that is not the property of Metergy, such as an team member-owned or vendor-owned computer.
Password	The unique password selected by a User that is required to log-on to the Metergy Network, a Mobile Device, laptop or IT Asset.
Policy	This Acceptable Use Policy.
Portable Storage Media	Any portable device has data storage function such as USB, CD, or Memory Cards.
Privacy Laws	Any provincial, federal, municipal or other laws, rules, regulations, judicial or administrative decisions or policies governing the collection, use, disclosure, storage of or access to personal information, as amended from time to time, including, without limitation, the *Personal Information and Protection of Electronic Documents Act*.
User(s)	Any person that uses the Metergy Network or an IT Asset, including directors, team members, and to the extent feasible, contractors, consultants, professional advisors, business partners and other third parties, authorized to connect to the Metergy Network. Note: A User can be an interface or service from another system.
Security Incident	Any of the following: • An unauthorized or unintended disclosure of Confidential Information, Password or other information prejudicial to Metergy, where such disclosure is made through Metergy Network; • misuse of an IT Asset or Metergy Network; detection of a virus, bypassing of anti-virus software or aborting of a virus scan; • any prohibited activity specified in section 4.8 of this Policy; any other violation of the IT Security Policy or this Policy.
SVP IT	Chief Customer Officer and Senior Vice President, IT
VPN	Virtual Private Network. A secure method of connecting to resources behind a firewall over public networks. Typical VPN connections will either be client-to-site in the case of mobile User VPN connections, or site-to-site in the case of intercompany or partner to company connections where multiple Users share and traverse the same VPN connection.
MDM	Mobile Device Management. A software service used for the administration of Mobile Devices, such as smartphones, tablets, laptops and desktop computers.

Appendix B: E-mail Requirements

PURPOSE:

E-mail requirements are intended to set out appropriate uses of Metergy’s e-mail accounts by Users.

1. Size limitations

a) Exceptions to the standard size of an e-mail account or maximum attachment size must be approved by the Vice President or L6 to whom the User requesting the exception reports.

2. Anti-Spam

a) Where an e-mail contains an executable file, archived file or other potentially dangerous attachment, such file or attachment will be blocked by the Metergy Network spam filter and the User will receive a prompt requiring User authorization prior to delivery of the E-mail.

b) Executable files, archived files or other potentially dangerous files that may be captured by the spam filter may be identified as ending in the following:
*.AD? *.BAT *.CRT *.HLP *.JS? *.MDE *.MSI *.PIF *.SCT *.VST
*.APP *.CHM *.CSH *.HTA *.KSH *.MDT *.MSP *.PRF *.SH?
*.VSW *.ASP *.CMD *.DLL *.INF *.LNK *.MDW *.MST *.REG
*.VB? *.WS? *.ASX *.COM *.EXE *.INS *.MDA *.MDZ *.OPS
*.SCF *.VSD *.ZIP *.BAS *.CPL *.FXP *.ISP *.MDB *.MSC *.PCD
*.SCR *.VSS

c) Electronic messages sent to promote any commercial activity are incompliance with the corporate Canadian Anti-Spam Policy.

3. Distribution lists and shared accounts

a) Shared accounts (for example, Metergy receptionist and helpdesk) and distribution lists must be approved by the responsible business unit Vice President or L6 and the SVP IT.

b) A shared account or distribution list request to the Metergy helpdesk must include the following information:

1) User names
2) Purpose
3) Expiry date, where applicable
4) Owner (User), specifically, the name, role and department
5) Access restrictions, as applicable

c) All updates to a shared account or distribution list must by authorized by the owner.

d) A distribution list included on the Metergy's Outlook Global Address Book must not contain any external or non-Metergy E-mail addresses

4. Account activation and deactivation

a) E-mail accounts will be limited to the following Users:
   1) Metergy team members
   2) Temporary or agency staff and personnel on contract with Metergy authorized by Human Resources, with a specified start date and end date

b) Human Resources will notify the IT Service Desk with requests for a new E-mail account or for deactivation of an existing E-mail account, for Users specified in Section 4(a) of this Appendix B.

c) Any exceptions to Section 4(a) of this Appendix B must be approved by the responsible business unit Vice President or L6 and the SVP IT.

d) All requests to access another User's account must be authorized by the responsible business unit Vice President and the SVP IT. Searches performed for the purposes of litigation will be authorized by the Chief Legal Officer.

5. Retention

a) E-mail will be automatically archived and purged following the retention schedule in Records Retention Policy.

b) An Outlook "deleted" E-mails folder will retain deleted E-mails for 30 days and will permanently delete such deleted E-mails after 30 days.

c) Unused E-mail accounts will be deactivated after 90 days, unless otherwise requested.

d) Unused E-mail accounts will be removed from the Metergy Network after 180 days, unless otherwise requested.