IT Security Policy

Metergy Solutions Inc.

Effective as of December 1, 2020.

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 is intended to manage and mitigate business and operational risk to the Metergy Network, IT Assets, Users and as otherwise contemplated in this Policy.

This Policy expands on the Code, and is intended to be read in conjunction with Metergy's Acceptable Use 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 authorized Users in the course of fulfilling their assigned duties and responsibilities. Users must access or retrieve stored information only as authorized or required in the course of their employment or contract and in accordance with this Policy.

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 Acceptable Use Policy and Metergy's other polices, Metergy may monitor the use of the IT Assets, review information and messages on the Metergy Network, and maintain 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 the security, management remains adequately funded. Executive management will ensure that policies align to Applicable Laws such as 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 team 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 and Metergy's other policies. 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 will store Information on Metergy Network drives, as instructed by an Information Owner, such as the applicable private and secure drive assigned to a division of Metergy. Failure to store Information on Metergy Network drives (such as local desktop or laptop drives) will render such Information unsecured and will result in the failure of such Information to be backed-up on a regular basis by IT.

4.3. Users will exercise precautions when sending or receiving Information over the Metergy Network for the purpose of preventing viruses and other potentially damaging software from compromising the Metergy Network and must comply with the anti-virus requirements set out in Appendix C to this Policy. Such precautions include password-protecting or encrypting Confidential Information, as prescribed.

4.4. Users are prohibited from undertaking actions intended to introduce or disseminate malicious software on the Metergy Network, such as viruses, worms, Trojan horses, or e-mail bombs. For certainty, such actions will be interpreted as misuse of the Metergy Network, amount to a Security Incident and will attract disciplinary action.

4.5. Users will ensure all IT Assets are password-protected and that any Non-Metergy IT Assets that are used for Metergy business purposes and store Information are also password-protected, where the password must comply with the Password Requirements set out in Appendix B to this Policy. Any use of Non-Metergy IT Assets for Metergy business purposes must be in compliance with all related Metergy policies and procedures.

4.6. Users will be prompted by notices generated by IT to select and change a Password at least every 90 days. The Password must comply with the Password Requirements set out in Appendix B to this Policy.

4.7. Users will maintain the confidentiality of their unique Password. Where a User suspects that a Password has been compromised, the User will promptly report the Security Incident to IT.

4.8. Users will contact the IT Service Desk for instructions on how to decrypt or decompress encrypted, compressed or password-protected files and scan such files for viruses (encrypted, compressed or password-protected files cannot be scanned by standard anti-virus software and must be manually scanned for viruses).

4.9. Users are prohibited from configuring, reconfiguring or otherwise modifying anti-virus software on the Metergy Network. Users are further prohibited from taking measures to bypass anti-virus software or abort anti-virus scans on the Metergy Network. For certainty, such actions will be interpreted as misuse of the Metergy Network, amount to a Security Incident and will attract disciplinary action.

4.10. Users will report any actual or suspected virus to IT immediately upon discovery of such actual or potential virus and are prohibited from undertaking efforts to remove the virus, unless otherwise directed by IT. Further, upon discovery of such actual or potential virus, the User will immediately cease use of the affected IT Asset and will physically turn it off, if possible.

4.11. Users will report lost or stolen IT Assets to IT immediately and their manager upon discovering the IT Asset has been lost or stolen.

4.12. Users will maintain and enforce physical security of IT Assets that contain Confidential Information by keeping such items in locked locations when not in use.

4.13. Users will report any actual or potential Security Incident to IT immediately upon discovery of such actual or potential Security Incident.

4.14. Users will not intentionally circumvent physical or logical safeguards.

4.15. Users will destroy all Information on Non-Metergy IT Assets upon termination of employment or as otherwise directed by Metergy.

5. IT Obligations

5.1. IT will monitor the Metergy Network for Security Incidents and other suspicious activity that could potentially compromise security.

5.2. IT will enforce Password security, in accordance with the Password Requirements set out in Appendix to this Policy.

5.3. IT will monitor remote access to Metergy Networks and will, in its sole discretion, grant access rights to the Metergy Network from outside the firewall, where business needs require such access.

5.4. IT will monitor remote access to ensure that all connections between computers on and outside the Metergy Network are secure.

5.5. IT will isolate the Metergy Network from public internet access.

5.6. IT will install security updates and patches to the Metergy Network and will monitor the Metergy Network to ensure all computers receive and apply any security software updates and patches.

5.7. IT will impose limited or privileged access rights on Users as directed by an Information Owner and will monitor such limitations and privileges for abuse.

5.8. IT may disconnect or otherwise remove an IT Asset from the Metergy Network, with or without advance notice to the User, in response to a Security Incident or as otherwise required to protect the security and integrity of the Metergy Network.

5.9. IT will revoke User access to the Metergy Network immediately following termination of employment or, in the case of a contractor or third party, immediately upon the cessation of contractual relations. User’s manager (or vendor/contractor manager) must recover all IT Assets and decide if e-mail address should be retained or deleted.

5.10. IT may limit or suspend User access rights, as directed by an Information Owner, where the User has taken a leave of absence. While on leave of absence, User may keep the IT Assets at the discretion of their manager.

5.11. IT will back-up all Metergy Network drives on a regular basis.

5.12. IT will configure all anti-virus software on the Metergy Network.

5.13. IT will update anti-virus software files weekly, or more frequently as required, or as precipitated by a Security Incident.

5.14. IT will maintain and enforce physical security of the Metergy Network by limiting access to areas where operational assets and IT Assets are stored.

5.15. IT will securely and completely remove all Information from IT Assets prior to disposal or resale of such IT Assets.

5.16. IT will review, classify and report on all Security Incidents, where risk to Metergy will be assessed and where report will be escalated to the President.

5.17. IT may impose restrictions on use of Non-Metergy IT Assets, such as restrictions on access to the Metergy Network, at the sole discretion of the SVP IT, with notice to Users.

5.18. IT will comply with the IT Administrator requirements set out in Appendix D to this Policy.

6. Exceptions

When compliance with this Policy cannot be achieved either partially or in full, a risk waiver is required. This must include an assessment of the risks presented by non-compliance, a justification for the deviation and proposed risk mitigation strategy and a time scale for review.

The risk waiver must be approved by the President with recommendation from the SVP IT.

7. Related Policies

7.1. IT Acceptable Use Policy
7.2. Ransomware Payment Policy
7.3. Code of Business Conduct

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.
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.
Information Owner	An Metergy team member designated by a member of Metergy Executive and that is responsible for setting and managing access rights to private and secure Metergy Network drives assigned to an Metergy group, division or other organizational unit.
IT	The Information Technology group, forming part of Metergy.
IT Administrator	A member of IT or a User authorized by the SVP IT or delegates to have specialized Metergy Network privileges.
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, laptops, smart phones (Blackberry, iPhone or Android), personal digital assistants (PDAs), tablet computers, combination tablet laptops and portable storage devices.
Non-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 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 Metergy Network.
Policy	This IT Security Policy.

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.
SVP IT	Chief Customer Officer and Senior Vice President, IT
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 sections 4.4, 4.7 and 4.9 of this Policy; • any other violation of the Acceptable Use Policy or this Policy.

Appendix B: Password Requirements

PURPOSE

Passwords are intended to protect the Metergy Network, IT Assets, Non-Metergy IT Assets (as applicable) and Information by limiting access rights to Users.

1. Passwords randomly generated by IT must be changed by the User immediately after first time use.

2. Passwords selected by Users must comply with the following requirements:

a) Contain at least seven characters, comprised of characters from at least three of the four categories:

1) Uppercase letters (A through Z).
2) Lowercase letters (a through z).
3) Base 10 digits (0 through 9).
4) Non-alphanumeric characters (such as exclamation point (!), dollar sign ($), number sign (#), etc.).

b) Not be a word in any language.

c) Not based on identifiable information about the User (such as birthday, family member names, etc.).

d) Composition of Mobile Device Password is exempted from the above requirements. See Appendix F to this Policy for Mobile Device Security Requirements.

3. Passwords must be encrypted if contained in e-mail or other form of electronic communication, or stored on an Metergy Network drive. Contact the IT helpdesk for instructions on how to encrypt a password.

4. Where a User fails to enter the correct Password after five consecutive unsuccessful attempts, a new Password may be required to access the Metergy Network.

5. Passwords must be reset by Users, including IT Administrators, at least every 90 days in accordance with section 4.6 of this Policy and section 10 of Appendix D to this Policy.

Appendix C: Anti-Virus Requirements

PURPOSE

Anti-virus software is intended to protect the Metergy Network and IT Assets by preventing, detecting, containing, and removing any viruses or malicious software from the Metergy Network.

1. All IT Assets or Non-Metergy IT Assets authorized to connect to the Metergy Network must be free of viruses and have functional anti-virus software as approved by IT and installed with the latest virus signature updates. Any use of Non-Metergy IT Assets to connect to the Metergy Network must be in compliance with all related Metergy policies and procedures.

2. All User e-mails, including any attachments, will be automatically scanned for viruses when being sent or received on the Metergy Network.

3. All electronic files, including encrypted files, stored on external devices, such as USB key or compact disk, must be scanned for viruses and must be certified as virus-free, prior to delivery to or after receipt from a third party or used inside the Metergy Network. Contact the IT helpdesk for instructions on how to scan external devices for viruses.

Appendix D: IT Administrator Requirements

PURPOSE

IT Administrator access requirements are intended to create accounts with specialized administrative privileges for the purpose of managing the IT obligations set out in Section 5 (IT Obligations) of this Policy. All IT Administrators and related privileges are subject to the sole discretion and oversight of the SVP IT or delegate. Delegation of the SVP IT's authority to a delegate will be temporary (in the absence of the SVP IT) and will only be granted to an IT manager.

1. By accepting the role of IT Administrator, the IT Administrator acknowledges and agrees to enforce this Policy and to monitor and mitigate risk to Metergy as contemplated by this Policy.

2. IT Administrators will be subject to an approval process prior to being granted such IT Administrator privileges and may be subject to a probationary period, in each case at the sole and exclusive discretion of the SVP IT or delegate.

3. Special administrative or managerial privileges to the Metergy Network will be reviewed and approved by the SVP IT or delegate prior to being granted on a least privilege basis to IT Administrators.

4. The SVP IT or delegate will undertake reasonable efforts to segregate distinct administrative and managerial privileges and grant such distinct administrative and managerial privileges to different IT Administrators for the purpose of mitigating potential misuse of such special administrative or managerial privileges.

5. IT Administrators and related privileges will be subject to review from time to time to ensure such IT Administrators and related privileges remain current, appropriate and necessary.

6. IT Administrators will only be granted the administrative and managerial privileges necessary to perform the duties identified by the SVP IT or delegate and such privileges may be expanded, restricted or suspended at the sole discretion of the SVP IT or delegate, with or without notice to the IT Administrator.

7. IT Administrators will use logging mechanisms, whenever possible, to record the exercise of special administrative or managerial privileges for the purpose of mitigating potential misuse of such special administrative or managerial privileges.

8. Any IT activities designated as "critical" by the SVP IT or delegate or an Information Owner will require more than one IT Administrator to execute and complete such critical activities.

9. IT Administrator accounts will comply with the Password requirements set out in Appendix A, will be unique to each IT Administrator, and must not be shared.

10. All IT Administrators must reset Passwords at least every 90 days and immediately upon departure of an IT Administrator.

Appendix E: Third-Party (Non-Employee) User Access Requirements

PURPOSE

Third-party (non-employee) User access requirements are intended to impose additional security requirements on designated Users for the purpose of protecting the integrity of the Metergy Network. For certainty, this Appendix E is intended to capture Users on short-term assignment to Metergy, third- party maintenance providers, or other Users identified by an Information Owner, IT Administrator or SVP IT or delegate.

1. Any User subject to this Appendix E will be required to read, acknowledge and agree to this Policy and other Metergy policies identified by the authorizing Information Owner, IT Administrator or SVP IT or delegate, prior to being granted access rights to the Metergy Network.

2. Any User subject to this Appendix E will be permitted to connect to the Metergy Network at an IT-issued workstation only. Any User subject to this Appendix E will be prohibited from connecting a Non-Metergy IT Asset to the Metergy Network, unless authorization to connect is granted by the SVP IT.

3. The authorizing Information Owner, IT Administrator or SVP IT or delegate will determine whether a User subject to this Appendix E will be assigned an Metergy e-mail account or be permitted remote access rights to the Metergy Network.

4. Where the User subject to this Appendix E is a third-party maintenance provider, the User authorization by an Information Owner, IT Administrator or SVP IT or delegate will be accompanied by an Metergy-issued helpdesk ticket reference number.

Appendix F: Mobile Device Security Requirements

These Mobile Device Security Requirements are applicable to all Mobile Devices.

Note: These requirements do not apply to Mobile Devices owned by customers or the general public, used to access publicly facing services and applications that do not contain Confidential Information.

Mobile Device security requirements are intended to impose additional security requirements on designated Users and Mobile Devices for the purpose of protecting the integrity of the Metergy Network as well as its Mobile Devices. Any User utilizing a Mobile Device is subject to this Appendix F.

1. Any User subject to this Appendix F will be required to read, acknowledge and agree to this Policy and other Metergy policies identified by the authorizing Information Owner, IT Administrator or SVP IT or delegate, prior to being granted rights for the Mobile Device to access the Metergy Network.

2. Any User subject to this Appendix F will be permitted to connect to the Metergy Network utilizing an approved and authorized Mobile Device only. Any User subject to this Appendix F will be prohibited from connecting a Non-Metergy Mobile Device to the Metergy Network, unless authorization to connect is granted by the SVP IT.

3. Metergy-owned Mobile Devices, including removable media, should be encrypted to minimize the potential risk of data loss. Encryption password strength should be commensurate to the level of risk associated with unauthorized access to the unencrypted data and meet Metergy's security requirements.

4. Access control security mechanisms must be in place to only allow approved Mobile Devices and Users to access the Metergy Network.

5. Users must not be assigned privileges which allow them to disable, amend or bypass approved technical controls and security configurations for accessing the Metergy Network.

6. Users accessing the Metergy Network via Mobile Devices must be uniquely identifiable through the use of registered and authorized User accounts.

7. Approved access control mechanisms must be established to prevent unauthorized access to the Metergy Network. Authentication mechanisms must be in line with Metergy approved standards and commensurate to the level of risk associated with unauthorized access to the Metergy Network.

8. Access control mechanisms should enforce auto-lock out or session timeout following a pre-defined period of inactivity, requiring Users to re-authenticate with their credentials.

9. Access rights for Mobile Devices will be assigned on a least privilege basis;

configured in such a way that Users are only able to access approve Metergy Network resources that are required for the Users to perform their roles.

10. Metergy-owned Mobile Devices remain the property of Metergy throughout their lifecycle unless otherwise agreed by Metergy. A formal process must be in place to inventory and establish ownership for all Metergy-owned Mobile Devices assigned to Users. The process should ensure that the inventory is a true reflection of all Metergy-owned Mobile Devices.

11. Mobile Devices consuming or requiring commercial licenses to enable Users to perform their roles (i.e. through access to the Metergy Network, locally installed approved applications or utilization of vendor provided device configuration and functionality) must be formally registered to ensure an accurate inventory of license obligations, consumption and potential liability is maintained.