MINIMUM SECURITY STANDARDS

Dated: 05/10/2018

A. Definitions. The following capitalized terms will have the following meanings whenever used in these Standards.

1. “Principle of Least Privilege” means restricting access rights to the minimum privileges necessary for an individual to perform his or her role;

2. “Privileged Account” means an account that has more authority and access to Customer networks, systems, information, and/or resources than a general account, including, without limitation, super-user, administrator, and root accounts;

3. “Demilitarized Zone (DMZ)” means a physical or logical subnetwork that separates Customer networks from other untrusted networks, including, without limitation, the Internet;

4. “Sandbox” means executing an application in a restricted operating system environment and limiting the application’s access to Customer networks, systems, information, and/or resources.

B. Minimum Security Standards.

CIT recognizes the ongoing threat of security incidents and breaches and the impact they can have on the stability and future of businesses large and small. With those threats in mind, CIT’s Customers must implement the following Minimum Security Standards (“Standards”) to protect themselves, their employees, and their clients.

1. Access Controls.

a. *Generally*. Customers must apply the Principle of Least Privilege to user, administrator, and system accounts.

b. *Device, Workstation, and System Access*.

(i) Passwords must be enabled on all workstations, mobile devices, and systems that can access Customer networks, whether in person or remotely;

(ii) Passwords must be complex and must consist of 12 characters or more. Complexity can be attained by combining uppercase and lowercase letters, by including special characters, and/or by using phrases;

(iii) Passwords must be set to expire at a minimum of every 90 days;

(iv) Passwords must not re-use any of the account’s last 10 passwords;

(v) Where possible, all accounts must have multi-factor authentication enabled. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics; and

(vi) Screen locks must be configured to limit access to unattended workstations.

c. *Network Access*.

(i) Privileged Accounts on Customer networks must restrict access to the minimum number of authorized individuals necessary;

(ii) Any publicly accessible system, including, without limitation, servers and internet of things (IOT) devices, must be isolated to a DMZ; and

(iii) Non-user utility accounts for network services, including, without limitation, scanning, printing, and e-faxing, must be restricted to the minimum necessary privileges.

d. *Remote Access*. Customers, their agents, employees, and contractors, must use secure and encrypted connections when accessing Customer networks, systems, information and/or resources across the Internet, or across unsecured or public networks (e.g. use of VPN for access, SFTP for transfers, encrypted wireless).

f. *Physical Access*.

(i) Workstations and servers must be physically secured in areas with restricted access; and

(ii) Mobile devices must be physically secured if left unattended.

2. System Protection.

a. *Patching*.

(i) Operating system and application services security patches must be installed in a commercially reasonable manner; and

(ii) Where patching is not possible for workstations and systems running custom applications, any such workstations and systems must be isolated on a DMZ or any such custom applications must be Sandboxed.

b. *Anti-Virus*.

(i) Anti-virus software, commercially adequate for the Customer’s system(s), must be installed and enabled on all mobile devices, workstations, and systems that are connected to Customer networks; and

(ii) Anti-virus software must be configured to update signatures daily.

c. *Firewall*.

(i) Customers must employ network-based firewalls, commercially adequate for the Customer's system(s), to protect their networks from unauthorized access;

(ii) Firewalls must be running and properly configured to block all inbound traffic that is not explicitly required for the intended use of the networks;

(iii) Firewalls must be configured to use geoblocking; and

(iv) Firewalls must incorporate an intrusion prevention system (IPS) and Gateway Anti-Virus.

d. *Mobile Devices*. For Customers with Bring Your Own Device (BYOD) policies, mobile devices must be configured for erase services, such that devices may be remotely wiped if lost, stolen, or upon employee termination.

3. Data Preservation. Customers must establish and follow a procedure to carry out regular system backups, which must comply with the following requirements:

(a) Backups must be performed at a minimum of every 24 hours;

(b) Backups must be verified at least monthly, either through automated verification, customer restores, or trial restores; and

(c) Backup media must be stored off-site and encrypted.

C. Violation of Minimum Security Standards.

Neither the Master Service Agreement nor these Standards requires that CIT take any action against any Customer violating these Standards, but upon written notice by CIT of any violation, CIT may immediately suspend its Services, and restrict Customer access as necessary, until such time as Customer can verify compliance with these Standards.

D. Revision of Minimum Security Standards.

CIT may change these Standards at any time by posting a new version on this page and sending Customer written notice thereof. The new version will become effective on the date of such notice.