SterlingRisk General I.T. Policy

1.0 Purpose

The following rules and guidelines are represent the overall policy related to use of Sterling's I.T. infrastructure. These guidelines are provided for the user's protection as well as the protection of the Information Systems owned by SterlingRisk

2.0 Scope

This policy applies to all SterlingRisk employees, contractors, vendors and agents using any I.T. related equipment connected to SterlingRisk's I.T. infrastructure in any way.

3.0 Policy

Software & Hardware Installation & Configuration

- In order to prevent unnecessary down time and ensure that all Sterling's PCs are operating correctly and efficiently, ALL software/hardware installations and configurations must be carried out by a member of the Sterling I.T. support staff. Absolutely NO software/hardware, either business related or otherwise, should be downloaded, installed, configured, or un-installed on or from ANY PC without the express consent and/or supervision of someone from the Sterling I.T. support staff. Client information and files should always be saved/stored on appropriately secured & backed up network file shares or databases, and should never be saved to your local PC or any removable storage device.

Communication

- The use of any Sterling company owned email accounts, telephones (hard wired or mobile), Internet connections, or any other communication software or devices owned by Sterling or connected to the company infrastructure are to be used solely for the purpose of conducting Company business. Sterling employees are responsible to ensure that they do not violate any SterlingRisk corporate policies, do not perform illegal activities, and do not use any of above mentioned devices or technologies for outside business interests. The SterlingRisk employee bears responsibility for the consequences should the access be misused.

Internet Usage

Internet use, on Company time, is authorized to conduct Company business only. Unauthorized Internet use brings the possibility of breaches to the security of confidential Company information, as well as creates the possibility of contamination to our system via viruses or spyware.

Email Usage

Under NO circumstances should personal email (ie: Gmail, Yahoo, AOL, etc) be used to conduct SterlingRisk business. Company confidential information must not be shared outside of the Company, without authorization, at any time. SterlingRisk email is also to be used for Company business only. You are also not to conduct personal business using the Company computer or email. Please keep this in mind as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste company time and attention, and in some cases can spread damaging spyware or viruses.

Ownership & Access
Keep in mind that all data (emails, files, voicemails, Instant Messages, etc) stored on Sterling owned I.T. equipment or services is the sole property of SterlingRisk. Management and other authorized staff have the right to access any of this data at any time. Please do not consider your electronic communication, storage or access to be private. Also, under no circumstances should any data stored on Sterling owned equipment or services be removed from these systems, or copied/forwarded or disseminated in any other way to any outside party without proper authorization.

Incident Reporting

- Should you witness or be suspicious of any action taken by any employee or other individual that you feel is in violation of any Sterling I.T. related policies, or is otherwise done with the intent of damaging or destroying any part of Sterling's I.T. infrastructure, you should report this to your immediate supervisor as well as to the Director of I.T. immediately. This includes any attempts to physically modify or damage Sterling owned equipment or technology, or to steal or illegally distribute any equipment, information or data that is the property of SterlingRisk.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I, ____________ ________ ___________ understand and agree to abide by this policy.

Print Name: ___________________ _____ Date:___________

Date	Version Number	Description of Revision(s) Made	Approval
06/06/2016	1.0	Initial Policy Revision	Michael Tampone - CTO
9/26/2018	1.1	Version/Date table added	Michael Tampone - CTO
10/10/2019	1.2	Annual Policy Review	Michael Tampone - CTO
10/14/2020	1.2	Annual Policy Review	Michael Tampone - CTO
11/1/2021	1.2	Annual Policy Review	Michael Tampone - CTO