SterlingRisk Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to SterlingRisk's network from any host. These standards are designed to minimize the potential exposure to SterlingRisk from damages which may result from unauthorized use of SterlingRisk resources. Damages include the loss of sensitive or confidential data, loss of intellectual property, damage to public image, damage to critical SterlingRisk internal systems, etc.

2.0 Scope

This policy applies to all SterlingRisk employees, contractors, vendors and agents with a SterlingRisk-owned, personally-owned, or privately owned (ie: library, web-café, etc) computer or workstation used to connect to the Sterling network. This policy applies to remote access connections used to do work on behalf of SterlingRisk, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in or cable modems, Remote Desktop Access, Terminal Server access, VMWare access, frame relay, ISDN, DSL, VPN, SSH, etc. This policy replaces any previously implemented policies dealing specifically with remote access to Sterling's network.

3.0 Policy

3.1 General

1. It is the responsibility of SterlingRisk employees, contractors, vendors and agents with remote access privileges to SterlingRisk's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to SterlingRisk.

2. Any SterlingRisk employee requesting remote access must obtain permission from their immediate supervisor for such access. Any supervisor granting such approval must provide a business justification for such access, and must sign & date such approval (physically or electronically). Unless otherwise approved by a member of the Executive staff, SterlingRisk employees must be employed with Sterling for a minimum of 90 days in order to be approved for remote access privileges.

3. General access to the Internet for recreational use by the user through the SterlingRisk Network is not permitted. The SterlingRisk employee is responsible to ensure that they do not violate any SterlingRisk policies, do not perform illegal activities, and do not use the access for outside business interests. The SterlingRisk employee bears responsibility for the consequences should the access be misused.

4. For additional information regarding SterlingRisk's remote access connection options, including how to request or troubleshoot remote access, please refer to the Help Desk or contact Sterling I.T.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. At no time should any SterlingRisk employee, contractors, vendors or agents provide their connection information, login name, or login/email password to anyone, not even family members. At no time should ANY SterlingRisk data or files be downloaded or stored locally onto a SterlingRisk or personally owned computer or device. Any system connecting to the SterlingRisk network (whether Sterling or personally owned) is to be used strictly as a means to establish a remote link to a system or host

running inside of the corporate network. NO SterlingRisk network or system passwords should be stored on any device used to connect to the SterlingRisk corporate network.

2. SterlingRisk employees, contractors, vendors and agents with remote access privileges are required to use a Two-Factor authentication protocol (currently Duo security) to authenticate access to the SterlingRisk internal network. The SterlingRisk I.T. department reserves the right to update or change the specific Two-Factor authentication protocol at any time.

3. SterlingRisk employees, contractors, vendors and agents with remote access privileges must ensure that their SterlingRisk-owned or personal computer or workstation, which is remotely connected to SterlingRisk's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user (and if the personal network is wireless, it MUST be protected with a secure password). Any network modem(s)/router(s) being used to connect to the SterlingRisk network must be secured, and accounts with access to this equipment must NOT be using the default password.

4. SterlingRisk employees, contractors, vendors and agents with remote access privileges to SterlingRisk's corporate network must not use non-SterlingRisk email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct SterlingRisk business, thereby ensuring that official business is never confused with personal business.

5. Using remote equipment for the purpose of split-tunneling or dual homing is not permitted.

6. All hosts that are connected to SterlingRisk internal networks via remote access technologies must have up-to-date anti-virus software installed and running, and a current anti-virus/anti-spyware definitions subscription from a reputable anti-virus software provider (such as Symantec), this includes personal computers.

7. All hosts that are connected to SterlingRisk internal networks via remote access technologies must have the latest Microsoft (or other OS & critical software) security & Operating System patches.

8. Organizations or individuals who wish to implement non-standard Remote Access solutions to the SterlingRisk production network must obtain prior approval from the Sterling I.T. Department.

9. Any expense required to modify a non-Sterling owned personal computer or device in order to meet the remote access requirements is the responsibility of the owner.

10. The Sterling I.T. department is not responsible for troubleshooting or providing support for any non-Sterling owned equipment or third-party connection issues. It is the responsibility of the user to contact the appropriate vendor or service provider to resolve any issues that are determined to be related to, or caused by, non-Sterling owned equipment or third party vendors.

11. Any remote access user agrees to immediately report to the Sterling Information Technology Department, the Human Resources department, and his/her manager any incidents or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

12. The Sterling Information Technology Department reserves the right to disable, without notice, any access to the network that puts the company’s systems, data, users, or clients at risk.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any contractors, vendors and agents found to have violated this policy may be subject to breach of contract, contract termination or other legal ramifications.

I, _____ _____ _____ understand and agree to abide by this policy.

Print Name: _____ _____ Date:_____

Date	Version Number	Description of Revision(s) Made	Approval
01/26/2016	1.0	Initial Policy Revision	Michael Tampone - CTO
10/3/2016	1.1	Modified Requirements Section	Michael Tampone - CTO
9/26/2018	1.2	Version/Date table added	Michael Tampone - CTO
10/28/2019	1.3	Annual Review	Michael Tampone - CTO
10/14/2020	1.4	Annual Review and update	Michael Tampone - CTO
11/01/2021	1.4	Annual Review	Michael Tampone - CTO