Policy Name: Remote Access Customer Network Policy

Document ID: IMS-00120

Revision: 1

Contents

1. Purpose

The purpose of this policy is to establish a framework for remote access to ST Engineering iDirect customer's infrastructure to preserve the best interests of ST Engineering iDirect's customers and ST Engineering iDirect for business continuity, corporate identity, and profitability.

2. Scope

This policy is applicable to all personnel working on behalf of ST Engineering iDirect in compliance with the Employee Policy Manual. The terms of this policy shall remain in force in perpetuity from the date an individual or organization's engagement begins with ST Engineering iDirect.

3. Policy Ownership and Review

All entities governed by the overarching Information Security Policy are subject to the referenced roles and responsibilities in addition to those specifically stated within this supporting policy.

This policy is owned by the Chief Information Security Officer ("CISO") and implemented by the Security Analyst.

4. Related Policy and Other Documentation

- Password Policy (IMS-00121)
- Manage Remote Access Customer Network (IMS-00139)
- Remote Support tools (maintained within Confluence Information Security space)

5. Terms and Definitions

Term	Definition
Authorized Personnel	Individuals who act on behalf of ST Engineering iDirect which may include employees, consultants, contractors, vendors, temporary personnel.
Event	Any episode when ST Engineering iDirect accesses customer network or infrastructure with explicit permission of the customer.

Employee Policy Manual	Internally published document ensuring that ST Engineering iDirect Employees understand their respective roles, responsibilities, and requirements to do so and the policies that govern them.

6. Policy

6.1 Any individual accessing customer infrastructure on behalf of ST Engineering iDirect is required to have a ST Engineering iDirect user account and have access to this policy.

6.2 Remote access is requested to the customer's Infrastructure only when absolutely required, after exhausting other available methods. Customers are responsible for determining how their infrastructure is accessed, what systems are accessed and in what timeslot they can be accessed. ST Engineering iDirect is responsible for documenting the customer approval, details, and timeslot in writing in an auditable manner, such as logging the applicable approval in the customer support portal.

6.3 If a customer provides ST Engineering iDirect with any log-in credentials to their infrastructure, it is the customer's responsibility to manage these passwords in line with their own password policy and to revoke access when the allotted timeslot for the authorized activity has expired.

6.4 The recommended method of accessing a customer's infrastructure is through one of the Remote Support tools preapproved by the CISO and published on a curated Acceptable Tooling list. The subjects of this policy are responsible for downloading and using only the appropriately licensed version of any tools on the remote support tools list.

6.5 In the event customers are unable to implement the remote access methods described above in Section 6.4, ST Engineering iDirect may be able to access a customer's infrastructure with their explicit permission, through a direct Internet connection or through other means such as a VPN connection. ST Engineering iDirect will make reasonable efforts to support this alternative method of remote access; however persistent connections such as site to site VPN tunnels are prohibited without explicit permission from the CISO.

6.6 ST Engineering iDirect Authorized Personnel will be required to request access credentials for each Event where remote access is required. It is ST Engineering iDirect's intent to safely store credentials according to our password policy for access to customer's infrastructure or remote access tools if required.

6.7 The customer is responsible to actively monitor the ST Engineering iDirect Authorized Personnel during all remote access Events.

6.8 Once the Event is complete, ST Engineering iDirect Authorized Personnel will log out and disconnect the session and the customer shall do the same.

6.9 Regardless of the method used for remote access, customers are requested to change access credentials after each use in accordance with security best practices.

7. Compliance

7.1. Compliance Measurement

As noted in the Employee Policy Manual, ST Engineering iDirect may at any time make exceptions to its policies and may change or revise some or all its policies, with or without prior notice to employees. This policy will be updated to reflect those changes in accordance with the Employee Policy Manual guidelines. ST Engineering iDirect requires its employees to acknowledge the Employee Policy Manual annually. This policy is available on the corporate intranet as well as the public website. The ST Engineering iDirect Authorized Personnel will be notified when policy adjustments are made through updates to the Policy Document Management System.

7.2. Exceptions

Any exception to the policy must be approved by the policy owner (as referenced in Section 3 above) in advance.

7.2.1. Known exceptions

There are occasions where our customers require named user accounts to allow remote access into their network. This causes delays in getting support while these specifically named accounts are created. To that end there is a permanent exception to this policy where a customer requires named accounts, and the accounts are protected by a 2nd authentication method. In this scenario credentials provided by the customer are maintained in the same way an ST Engineering iDirect employee manages their own credentials. A list of customers with known exceptions is maintained on the Information Security Confluence page.

7.3. Non-compliance

An ST Engineering iDirect personnel found to have violated this policy may be subject to disciplinary action.

8. Version Management

8.1. Document Change Log

The full version history of this document is part of the metadata of this document stored in SharePoint. Contact GlobalPerformance@idirect.net with any questions.

8.2. Review and Approval Responsibilities

Function	Responsibility
Security Analyst	Author/Owner
ISMS Officer	Reviewer
Manager Global IT Operations	Approver
Information Security Manager	Approver
Vice President Customer Success	Approver
Responsibilities = Author, Owner, Reviewer(s), and Approver	

Review and approvals are electronically maintained in the DMS.