**Remote Access Policy**

Prepared By

**IT Security**

 **VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author/Editor** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

**PURPOSE 4**

**SCOPE 4**

**OBJECTIVE 4**

**POLICIES 5**

**ENFORCEMENT 7**

1. **PURPOSE**

Remote access to the Organization Group systems would always pose risks to the Group regardless of any security measures put in place. Hence, the purpose of this policy is to define standards for connecting to the group’s network from any host. These standards are designed to minimize the potential exposure to the group from damages, which may result from unauthorized use of the group resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical group internal systems, etc.

2. **SCOPE**

This policy applies to all Organization Group employees, contractors and vendors with corporate owned computers or workstations used to connect to the Group’s network. This policy applies to remote access connections used to do work on behalf of the Group, including reading or sending email, viewing intranet web resources and network/system/application support.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, Internet, ISDN, ADSL, VPN, and SSH etc.

***This policy covers all methods of access, wired and wireless data communication.***

***3. OBJECTIVE***

***The main objective of this policy is to allow Organization IT Support staff, selected vendors and approved business users to access Organization resources through remote access. The current infrastructure through e-Citrix technology allows remote access to Organization’s enterprise application system.***

4. **POLICY**

4.1 **General**

1. ***It is the responsibility of the Organization requester’s and approver’s with remote access privileges to the corporate network to ensure that their access privileges should be less or minimal necessary to carry out the functions.***
2. ***General access to the Internet for recreational use by the user through the Group’s network is not permitted. It is the users' responsibility to comply with the Group’s policies and the responsibility of the Level 2 manager to ensure that staff with remote access privileges is comply with Organization Group’s policies.***

4.2 **Requirements**

* + - 1. All remote access connections must be strictly controlled. Controls will be enforced via one-time password authentication (e.g. Vasco tokens and eCitrix id).
			2. ***Users with remote access privileges must ensure that their computer Windows Firewall setting shall be turned on and running at all times when connecting to Organization Group. Windows Firewall helps to protect the computer by preventing unauthorised users from gaining access to the computer through the internet.***
			3. No dial-in access shall be permitted to bypass Organization Group firewall.
			4. At no time should any user share his or her login or password to anyone else including family members. Two factor authentication devices (e.g. hardware tokens or smart cards) must not be shared under any circumstances.

***Users with remote access privileges must ensure that all authentication devices (e.g. hardware tokens or smart cards) must return to IT Security once task completed or the privileges has been revoked. IT Security must ensure that all returned devices are recorded before reassigned the devices to others.***

* + - 1. Users with remote access privileges must ensure that their computer or workstation, which is remotely connected to the Organization group’s network, is not connected to any other network at the same time. ***User must ensure to disabled and disconnect other network except for Organization network.***
			2. Routers for dedicated ISDN lines configured for access to the group’s network must meet minimum authentication requirements of CHAP.
			3. Configuration of split-tunnelling or dual homing is not permitted at any time.
			4. Unauthorized personal computer or cyber cafe’s computers are prohibited from connecting to the group’s network.
			5. Users will be automatically disconnected from the network after fifteen minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes cannot be used to keep the connection active.
			6. Organizations or individuals who wish to implement non-standard Remote Access solutions to the group production network must obtain prior approval from IT Security.
			7. ***It is the responsibility of the manager to ensure staff that is given remote access based on the "need to have" principle.***
			8. ***All cost has to be borne by the requestor’s respective cost centre.***

4.3 ***Refer to guideline “2.015 : Guideline on Hardware Token for Organization Internal User Remote Access”, if token is required.***

4.4 ***The completed and approved form (Refer to Guideline on Remote Access Requirement) to be forwarded to CSC together with the Service Request (SR) for further action.***

4.5 **Eligible Remote Access Users**

***The following types of users are allowed remote access.***

***Organization IT Support staff.***

***Organization Business Users.***

***Application Users of application.***

***Others that have been granted approval by Organization IT Management***

4.6 **IT Remote Support Service**

1. IT Support staff are allowed remote access for applications for support purposes. IT Managers are advised to allow remote access only on a ***"need to have"*** basis based on Classification of Business Functions in Appendix A.

1. IT Remote Support Services is allowed for application with business function that has been classified as ***"Very Critical"*** and ***"Critical"***.
2. IT Remote Support Services should not be provided for application with business function that has been classified as ***"Required"*** or ***"Non-Critical"***. IT Security does not recommend remote support services for such applications to reduce the Groups' exposure to unnecessary outside threats. However, such application may be allowed remote support services on an ad-hoc basis for a limited time period and approved by the Organization IT Management.
3. All IT Remote Support Services staff must use a token and a Group issued personal computer (if provided) when doing remote access support.

4.7 **Remote Access for Applications**

a) All application requiring remote access must obtain approval from Organization IT Management. ***Refer to Guideline on Remote Access Requirement for more information on the request form. The form must include comments, review and approval from various section (e.g Application Owner, IT Security, Network Services and IT Management).***

b) Once an application has obtained approval from management, the following controls must be in place:

i- Selected approved users must be provided with tokens

ii- Selected approved users must be issued with remote access User IDs.

***iii- Identified controls should be in place. (e.g Organization Desktop policy, Antivirus policy, Internet Usage policy and Remote Access policy)***

c) ***Any deviation from the above controls must be approved by IT Security and Organization IT Management.***

4.8 **Revocation of Remote Access Capability**

1. It is the responsibility of the Level 2 manager to ensure remote access is removed immediately upon termination of duties or resignation of a staff. The manager's must ensure that the remote access administrator is informed IMMEDIATELY upon receiving such information.

b) Level 2 Manager is responsible to fill up the **“Resignation Checklist Form (Appendix 2)**” under Business HR (HCM) SPI policies for resignation of staff or termination of duties.

1. Remote access administrator must ensure that the staff's remote access capability is removed immediately.

5. **ENFORCEMENT**

# 5.1 All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.

# 5.2 Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.

5.3 Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.

5.4 Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.