Acceptable Use Policy

Last Update Status: *Updated October 2022*

1. Overview

Rhytha Web Solutions Pvt Ltd is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Rhytha Web Solutions Pvt Ltd . These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Rhytha Web Solutions Pvt Ltd employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at Rhytha Web Solutions Pvt Ltd . These rules are in place to protect the employee and Rhytha Web Solutions Pvt Ltd . Inappropriate use exposes Rhytha Web Solutions Pvt Ltd to cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Rhytha Web Solutions Pvt Ltd business or interact with internal networks and business systems, whether owned or leased by Rhytha Web Solutions Pvt Ltd , the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Rhytha Web Solutions Pvt Ltd and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Rhytha Web Solutions Pvt Ltd

policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Rhytha Web Solutions Pvt Ltd , including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Rhytha Web Solutions Pvt Ltd .

4. Policy

4.1 General Use and Ownership

4.1.1 Rhytha Web Solutions Pvt Ltd proprietary information stored on electronic and computing devices whether owned or leased by Rhytha Web Solutions Pvt Ltd , the employee or a third party, remains the sole property of Rhytha Web Solutions Pvt Ltd . You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Rhytha Web Solutions Pvt Ltd proprietary information.

4.1.3 You may access, use or share Rhytha Web Solutions Pvt Ltd proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Rhytha Web Solutions Pvt Ltd may monitor equipment, systems, and network traffic at any time, per Infosec's *Audit Policy*.

4.1.6 Rhytha Web Solutions Pvt Ltd reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a Rhytha Web Solutions Pvt Ltd email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Rhytha Web Solutions Pvt Ltd , unless posting is during business duties.

4.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Rhytha Web Solutions Pvt Ltd authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Rhytha Web Solutions Pvt Ltd -owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Rhytha Web Solutions Pvt Ltd .
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Rhytha Web Solutions Pvt Ltd or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting Rhytha Web Solutions Pvt Ltd business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Rhytha Web Solutions Pvt Ltd computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Rhytha Web Solutions Pvt Ltd account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Rhytha Web Solutions Pvt Ltd network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Rhytha Web Solutions Pvt Ltd employees to parties outside Rhytha Web Solutions Pvt Ltd .

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Rhytha Web Solutions Pvt Ltd 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Rhytha Web Solutions Pvt Ltd or connected via Rhytha Web Solutions Pvt Ltd 's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging or posting to social media platforms by employees, whether using Rhytha Web Solutions Pvt Ltd ’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Rhytha Web Solutions Pvt Ltd ’s systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Rhytha Web Solutions Pvt Ltd ’s policy, is not detrimental to Rhytha Web Solutions Pvt Ltd ’s best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from Rhytha Web Solutions Pvt Ltd ’s systems is also subject to monitoring.
2. Rhytha Web Solutions Pvt Ltd ’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>’s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Rhytha Web Solutions Pvt Ltd and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Rhytha Web Solutions Pvt Ltd ’s *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to Rhytha Web Solutions Pvt Ltd when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Rhytha Web Solutions Pvt Ltd . Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Rhytha Web Solutions Pvt Ltd ’s

trademarks, logos and any other Rhytha Web Solutions Pvt Ltd intellectual property may also not be used in connection with any blogging or social media activity

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam
- Ransomware

Server Security Policy

Last Update Status: *Updated October 2022*

8. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

9. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Rhytha Web Solutions Pvt Ltd . Effective implementation of this policy will minimize unauthorized access to Rhytha Web Solutions Pvt Ltd proprietary information and technology.

10. Scope

All employees, contractors, consultants, temporary and other workers at Rhytha Web Solutions Pvt Ltd and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Rhytha Web Solutions Pvt Ltd or registered under a Rhytha Web Solutions Pvt Ltd -owned internal network domain.

This policy specifies requirements for equipment on the internal Rhytha Web Solutions Pvt Ltd network. For secure configuration of equipment external to Rhytha Web Solutions Pvt Ltd on the DMZ, see the Internet DMZ Equipment Policy.

11. Policy

4.1 General Requirements

4.1.1 All internal servers deployed at Rhytha Web Solutions Pvt Ltd must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs, and approved by the InfoSec team. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the

configuration guides, which includes review and approval by InfoSec. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up to date.
- Configuration changes for production servers must follow the appropriate change management procedures

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved InfoSec team guidelines.

4.2.2 Services and applications that will not be used must be disabled where practical.

4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

4.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

4.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

4.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

4.2.8 Servers should be physically located in an access-controlled, secured environment.

4.2.9 Servers are specifically prohibited from operating from uncontrolled or unsecured cubicle areas.

4.3 Monitoring

4.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2 Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

12. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

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

13. Related Standards, Policies and Processes

- Audit Policy
- DMZ Equipment Policy

14. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

- De-militarized zone (DMZ)

Information Logging Standard

Last Update Status: *Updated October 2022*

15. Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

16. Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

17. Scope

This policy applies to all production systems on Rhytha Web Solutions Pvt Ltd Network.

18. Policy

4.1 General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

4.1.1 What activity was performed?

4.1.2 Who or what performed the activity, including where or on what system the 4.1.3 activity was performed from (subject)?

4.1.4 What the activity was performed on (object)?

4.1.5 When was the activity performed?

4.1.6 What tool(s) was the activity was performed with?

4.1.7 What was the status (such as success vs. failure), outcome, or result of the activity?

4.2 Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

4.2.1 Create, read, update, or delete confidential information, including confidential authentication information such as passwords;

4.2.2 Create, update, or delete information not covered in #1;

4.2.3 Initiate a network connection;

4.2.4 Accept a network connection;

4.2.5 User authentication and authorization for activities covered in #1 or #2 such as user login and logout;

4.2.6 Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;

4.2.7 System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;

4.2.8 Application process startup, shutdown, or restart;

4.2.9 Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network

bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and

4.2.10 Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

4.3.1 Type of action – examples include authorize, create, read, update, delete, and accept network connection.

4.3.2 Subsystem performing the action – examples include process or transaction name, process or transaction identifier.

4.3.4 Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.

4.3.5 Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.

4.3.6 Before and after values when action involves updating a data element, if feasible.

4.3.7 Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.

4.3.8 Whether the action was allowed or denied by access-control mechanisms.

Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

4.4.1 Microsoft Windows Event Logs collected by a centralized log management system;

4.4.2 Logs in a well-documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system;

4.4.3 Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and

4.4.4 Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

19. Policy Compliance

5.4 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.5 Exceptions
Any exception to the policy must be approved by the Infosec team in advance.

5.6 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

20. Related Standards, Policies and Processes
None.

21. Definitions and Terms
None.

Remote Access Policy

Last Update Status: *Updated October 2022*

22. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks the best of our ability.

23. Purpose

The purpose of this policy is to define rules and requirements for connecting to Rhytha Web Solutions Pvt Ltd 's network from any host. These rules and requirements are designed to minimize the potential exposure to Rhytha Web Solutions Pvt Ltd from damages which may result from unauthorized use of Rhytha Web Solutions Pvt Ltd resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Rhytha Web Solutions Pvt Ltd internal systems, and fines or other financial liabilities incurred as a result of those losses.

24. Scope

This policy applies to all Rhytha Web Solutions Pvt Ltd employees, contractors, vendors and agents with a Rhytha Web Solutions Pvt Ltd -owned or personally-owned computer or workstation used to connect to the Rhytha Web Solutions Pvt Ltd network. This policy applies to remote access connections used to do work on behalf of Rhytha Web Solutions Pvt Ltd , including reading or sending email and viewing intranet web

resources. This policy covers any and all technical implementations of remote access used to connect to Rhytha Web Solutions Pvt Ltd networks.

25. Policy

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

General access to the Internet for recreational use through the Rhytha Web Solutions Pvt Ltd network is strictly limited to Rhytha Web Solutions Pvt Ltd employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the Rhytha Web Solutions Pvt Ltd network from a personal computer, Authorized Users are responsible for preventing access to any Rhytha Web Solutions Pvt Ltd computer resources or data by non-Authorized Users. Performance of illegal activities through the Rhytha Web Solutions Pvt Ltd network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Rhytha Web Solutions Pvt Ltd networks to access the Internet for outside business interests.

For additional information regarding Rhytha Web Solutions Pvt Ltd 's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (<company url>).

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a Rhytha Web Solutions Pvt Ltd -owned computer to remotely connect to Rhytha Web Solutions Pvt Ltd 's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct Rhytha Web Solutions Pvt Ltd business must be approved in advance by InfoSec and the appropriate business unit manager.

4.1.5 All hosts that are connected to Rhytha Web Solutions Pvt Ltd internal networks via remote access technologies must use the most up-to-date anti-virus software (<place url to corporate software site here>), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

4.1.6 Personal equipment used to connect to Rhytha Web Solutions Pvt Ltd 's networks must meet the requirements of Rhytha Web Solutions Pvt Ltd -owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to Rhytha Web Solutions Pvt Ltd Networks*.

26. Policy Compliance

5.7 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.8 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.9 Non-Compliance

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

27. Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Rhytha Web Solutions Pvt Ltd ’s network:

- *Acceptable Encryption Policy*
- *Acceptable Use Policy*
- *Password Policy*
- *Third Party Agreement*
- *Hardware and Software Configuration Standards for Remote Access to Rhytha Web Solutions Pvt Ltd Networks*

Remote Access Tools Policy

Last Update Status: *Updated October 2022*

28. Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Rhytha Web Solutions Pvt Ltd network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on Rhytha Web Solutions Pvt Ltd computer systems.

29. Purpose

This policy defines the requirements for remote access tools used at Rhytha Web Solutions Pvt Ltd .

30. Scope

This policy applies to all remote access where either end of the communication terminates at a Rhytha Web Solutions Pvt Ltd computer asset.

31. Policy

All remote access tools used to communicate between Rhytha Web Solutions Pvt Ltd assets and other systems must comply with the following policy requirements.

4.1 **Remote Access Tools**

Rhytha Web Solutions Pvt Ltd provides mechanisms to collaborate between internal users, with external partners, and from non- Rhytha Web Solutions Pvt Ltd systems. The approved software list can be obtained from <link-to-approved-remote-access-software-list>. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

4.1.1 All remote access tools or systems that allow communication to Rhytha Web Solutions Pvt Ltd resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.

4.1.2 The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks such as OAuth 2.0. The remote access tool must mutually authenticate both ends of the session.

4.1.3 Remote access tools must support the Rhytha Web Solutions Pvt Ltd application layer proxy rather than direct connections through the perimeter firewall(s).

4.1.4 Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Rhytha Web Solutions Pvt Ltd network encryption protocols policy.

4.1.5 All Rhytha Web Solutions Pvt Ltd antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard Rhytha Web Solutions Pvt Ltd procurement process, and the information technology group must approve the purchase.

32. Policy Compliance

5.10 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.11 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.12 Non-Compliance

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

33. Related Standards, Policies and Processes

None.

34. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

- Application layer proxy

35. Revision History

Date of Change	Responsible	Summary of Change
June 2014	Rhytha Policy Team	Updated and converted to new format.
Oct 2022	Rhytha Policy Team	Updated and converted to new format.