VDI Usage and Security Policy

Version: 1.0

December 2024

(Privacy: Private**)**

DOCUMENT CONTROL

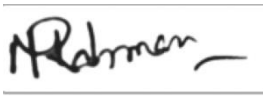
A. Document Information

Document Name	VDI Usage and Security Policy
Document Number	BS23-ISMS-POL-43
Document Author	Head of Quality & Compliance
Document Location and Access	This document will be maintained as an electronic copy in a storage/portal/file server and shared with the appropriate stakeholders according to the Document Distribution List by mail/portal/shared drive.
Document Control	This document is for the use of BS23. Any document sharing with external entities without the approval of the authority is strictly prohibited and is subjected to forward for disciplinary action for such activity. Any unauthorized modification is strictly prohibited. Please refer to the author/owner should there be any need for clarification or additional information about the document.
Document Classification	This document is classified as **'Private'**. Information/ document could be used/ disclosed with authorized persons according to document classification.
Conformity	Any practice deemed required by the Regulatory Body, Government, Relevant standard/ frameworks/ directives, and Applicable Local/ International Laws will override the entire or any part mentioned in this document.
Recommendation	Users of this document are responsible for using only the latest version.
Enforcement	This document shall be released and come into force with effect from the date of Approval.
Retention & Disposition	The obsolete version of the document will be retained and maintained according to the **Retention Policy** of BS23. The copies distributed among the users will be invalid immediately after the publication of the new version and respective department/Division/Branch Head will destroy the obsolete distributed.
Review Frequency	This document and the content statements of the document will be reviewed as on a demand basis.

B. Document Distribution List

Serial No.	Person/ Department/ Designation/ Team
01	All Internal Stakeholders

C. Author Information

Prepared By		
Name	**Designation**	**Signature**
Md. Sazzad Munir	Head of Quality & Compliance	
Reviewed By		
Name	**Designation**	**Signature**
Mizanur Rahman	CTO	
Approved By		
Name	**Designation**	**Signature**
Raisul Kabir	CEO	

D. Document History

Version No	Revision Date	Approval Date	A/M/ D/N	Description of Change	Document Author	Approved By
1.0	18-Dec-2024	24-Dec-2024	N	First release	Head of Q&C	CEO

* A= Added, M= Modified, D= Deleted, N= New Published

Table of Contents

1 Purpose

To establish best practices for the secure use of Virtual Desktop Infrastructure (VDI) to safeguard digital assets, ensure compliance with security standards, and provide a secure work environment for employees.

2 Scope

This policy applies to all employees, contractors accessing clients and company resources through VDI.

3 Responsibilities

- **IT Department**: Manage VDI configurations, implement security measures, monitor for compliance, and provide user training.
- **Users**: Follow access and usage guidelines, report security incidents, and maintain the confidentiality of credentials.

4 Provider-Specific Guidelines

4.1 VMware Horizon

- **Data Security**:
  - Use VMware NSX for micro-segmentation to isolate sensitive workloads.
  - Encrypt VDI traffic using VMware Unified Access Gateway (TLS/SSL).
- **Compliance**:
  - Enable vSphere Trust Authority to ensure workload integrity and compliance with standards like HIPAA and GDPR.
  - Monitor logs with VMware Aria Operations for Logs for compliance reporting.

4.2 Citrix Virtual Apps and Desktops

- **Data Security**:
  - Enable Secure Workspace Access to protect against unauthorized data exfiltration.
  - Use Citrix Analytics for Security to detect and prevent anomalies like unauthorized file sharing.
- **Compliance**:
  - Configure Citrix Cloud services to meet SOC 2, ISO 27001, and GDPR compliance.
  - Enable Citrix Content Collaboration for secure file handling and encrypted sharing.

4.3 Microsoft Azure Virtual Desktop (AVD)

- **Data Security**:
  - Enable Azure Defender for Cloud to monitor and protect VDI resources.
  - Restrict access using Conditional Access policies and Microsoft Defender for Identity.
- **Compliance**:
  - Leverage Azure Policy to enforce compliance with HIPAA, FedRAMP, and ISO 27001.
  - Store sensitive data in Azure regions that align with data sovereignty requirements.

4.4 AWS WorkSpaces

- **Data Security**:
  - Enforce encryption at rest using AWS KMS and in-transit using SSL/TLS.
  - Implement IAM roles and policies to enforce least privilege access.
- **Compliance**:
  - Utilize AWS Artifact to generate compliance reports for PCI DSS, SOC 2, or HIPAA.
  - Monitor with AWS CloudTrail and Amazon GuardDuty for real-time compliance insights.

5 Common Security Practices

5.1 Access Control

- Enforce multi-factor authentication (MFA) for all VDI logins.
- Implement role-based access control (RBAC) to limit access to resources based on job roles.
- Conduct periodic reviews of user access rights.

5.2 Security Configuration

- Use encrypted communication protocols (e.g., TLS/SSL) for VDI sessions.
- Disable copy-paste and USB redirection unless explicitly required and approved.
- Enable screen locking after a period of inactivity.
- Restrict installation of unauthorized software on virtual desktops.

5.3 Endpoint Security

- Ensure client devices accessing VDI meet minimum security requirements, including up-to-date antivirus and firewalls.
- Regularly patch and update VDI client software.

5.4 Data Protection

- Enforce data encryption at rest and in transit using provider-specific encryption mechanisms.
- Store sensitive files in centralized, secure locations within the VDI environment.
- Enable automated backups for critical data.
- Prevent file transfers from virtual desktops to local devices unless explicitly authorized.

5.5 Monitoring and Auditing

- Log all user activities and administrative actions within the VDI.
- Regularly audit VDI logs for anomalies or unauthorized access.
- Implement real-time alerts for potential security threats.

5.6 Incident Response

- Employees must report the incident to the IT team (it@brainstation-23.com), line manager and SBU/Department head immediately.
- Fill out the Incident reporting form: https://forms.office.com/r/6aXPjTxvQA

- .Temporarily revoke access for users involved in a suspected security breach.

5.7 Training and Awareness

- Conduct mandatory security training on VDI best practices before starting work in VDI.
- Provide ongoing updates about emerging threats and prevention techniques.

6 Compliance and Enforcement

- Non-compliance with this policy may result in disciplinary action, including termination of VDI access privileges.
- Regularly review and update this policy to align with evolving security threats and business needs.

7 Approval and Review

- This policy is subject to approval by the Information Security Team and will be reviewed annually or as needed.