DATAMOVER ACCEPTABLE USE POLICY

1. Purpose

This Acceptable Use Policy establishes the rules and guidelines governing the appropriate use of organizational information systems, data assets, and technology resources. This policy also incorporates comprehensive requirements for third-party information exchange agreements to ensure that all data sharing arrangements with external parties maintain adequate security controls and comply with applicable laws and regulations.

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, vendors, and other personnel who access, use, or manage organizational information systems and data. It also governs all arrangements involving the exchange, sharing, or transfer of information with third parties, including but not limited to business partners, service providers, government agencies, and affiliated organizations.

3. Definitions

Covered Information: Any data classified as confidential, restricted, or sensitive under the organization's data classification policy, including personal data, financial records, intellectual property, and trade secrets.

Critical Information: Data essential to business operations whose loss, corruption, or unauthorized disclosure could cause significant harm to the organization or its stakeholders.

Third Party: Any external organization, entity, or individual with whom the organization exchanges information, including vendors, partners, contractors, and regulatory bodies.

Information Exchange Agreement: A formal, documented agreement establishing the terms, conditions, and security requirements governing the sharing of information between the organization and a third party.

4. General Acceptable Use Requirements

4.1 Authorized Use

Users shall access organizational information systems and data only for legitimate business purposes consistent with their job responsibilities. All users must comply with applicable laws, regulations, and organizational policies when using technology resources.

4.2 Account and Password Management

Users are responsible for safeguarding their authentication credentials. Sharing of passwords or access tokens is prohibited. Users must immediately report suspected compromise of their credentials to the Information Security team.

4.3 Data Handling

Users must handle data in accordance with its classification level. Covered and critical information requires additional safeguards including encryption during transmission and storage, access restrictions, and proper disposal methods.

4.4 Prohibited Activities

The following activities are strictly prohibited:

- Unauthorized access to systems, networks, or data
- Installation of unauthorized software or hardware
- Circumvention of security controls or monitoring systems
- Transmission of malicious code or unauthorized data extraction
- Use of systems for illegal activities or harassment
- Unauthorized disclosure of confidential or proprietary information

6. Monitoring and Enforcement

6.1 Monitoring

The organization reserves the right to monitor, access, and review all information systems, networks, and data for security, compliance, and operational purposes. Users should have no expectation of privacy when using organizational resources.

6.2 Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, civil litigation, and criminal prosecution where applicable. Third parties found in violation of information exchange agreement requirements may be subject to contract termination and legal remedies.

7. Exceptions

Requests for exceptions to this policy must be submitted in writing to the Information Security Officer and require documented business justification. Approved exceptions must include compensating controls and are subject to periodic review.

8. Policy Review

This policy shall be reviewed annually or upon significant changes to the regulatory environment, business operations, or threat landscape. The Information Security Officer is responsible for initiating the review process and ensuring appropriate stakeholder involvement.