ACCESS CONTROL POLICY

1. Overview
In computer security, general access control includes identification, authorization, authentication, access approval, and auditing of staff access to computer resources.

2. Purpose
The purpose of this policy is to maintain an adequate level of security to protect JMT data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and ensure a secure and reliable operation of JMT information systems.

3. Scope
This policy applies to all JMT employees, contractors, vendors, and agents with JMT valid credentials for accessing JMT information systems resources. This policy applies whether the access is from JMT owned or personally-owned devices. It also applies to remote access connections to JMT information systems resources used to do work on behalf of JMT. This policy covers all technical implementations of access used to connect to JMT networks.

4. Policy
Only authorized users are granted access to information systems. Authorized users are limited to specific, defined, documented, and approved applications and levels of access rights. Computer and communication system access control is achieved via user IDs, which are unique to each individual user to provide personal accountability and traceability.

Who is Affected: This policy affects all employees of JMT and its subsidiaries, along with all contractors, consultants, temporary employees, and business partners with access privileges. Employees who deliberately violate this policy will be subject to disciplinary action—up to and including termination.

Affected Systems: This policy applies to all computer and communication systems owned, leased, rented, subscribed or operated by JMT and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

Entity Authentication: Any user (remote or internal) accessing JMT networks and systems must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes, but is not limited to:

- Unique user identifier
- At least one of the following:
  o Biometric identification
  o Password conforming to JMT Password Policy
Personal Identification Number
- A telephone callback
- Token or a multi-factor authentication method

**Workstation Access Control System:** All workstations used for JMT business activity must use an access control system approved by JMT information systems no matter where they are located. In most cases, this will involve password-enabled lock-out screens with a time-out-after-no-activity feature and a power-on-password for the central processing unit (CPU). Active workstations are not to be left unattended for prolonged periods of time. When a user leaves a workstation, that user is expected to properly log out or lock their workstation. Users will be held responsible for all actions taken after signing on. Where appropriate, inactive workstations will be locked after a period of inactivity (typically 15 minutes). Users will then be required to log back on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the user during the authorized user’s absence.

**Disclosure Notice:** Before signing in, a notice is displayed warning users that they can only access the system with the proper authority. The warning message will explain that the system is a private network or application and any unauthorized users should disconnect or log off immediately.

**System Access Controls:** Proper controls shall be in place to authenticate the identity of users and validate each user’s authorization before he or she can access information or services on JMT information systems. Data used for authentication shall be protected from unauthorized access. Controls will ensure that only personnel with proper permissions are allowed access; permissions will be applied to all computer-resident information based on concepts of Need to Know and Least Privilege. This ensures systems and information are not improperly disclosed, modified, deleted, or rendered unavailable.

**Access Approval:** System access will not be granted to any user without appropriate approval. Management must notify JMT’s Information Systems team immediately to report all significant changes in end-user duties or employment status. User access will be revoked immediately if the individual has been terminated. In addition, user privileges will be changed if the user is transferred to a different job or role.

**Limiting User Access:** JMT approved access controls will be used to limit user access to only those network applications, data and functions for which they have been authorized.

**Need-to-Know:** Users will be granted access to information on a “need-to-know” basis. That is, users will only receive access to the minimum applications and privileges required to perform their jobs responsibilities.

**Compliance Statements:** Users who access JMT’s information systems must sign a compliance statement outlining policies prior to issuance of a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by JMT policies and procedures related to computers and information systems. Annual confirmations will be required from all system users.

**Audit Trails and Logging:** All access is logged and monitored.

**Confidential Systems:** Access to confidential systems will be logged and audited.
Access for Non-Employees: Before any contractors, consultants or business partner is given access to JMT computers or information systems, the JMT information systems’ Contractor Access Request Form (located on the JMT intranet) must be completed and submitted by the requesting JMT manager with necessary approvals.

Unauthorized Access: Employees are prohibited from unauthorized access to any other information systems or damaging, altering, or disrupting the operations of these systems in any way.

Remote Access: Remote access must conform to the JMT Remote Access Policy.

5. Policy Compliance

Compliance Measurement: JMT’s Information Security team (InfoSec) will verify compliance to this policy through various methods including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspections. InfoSec will also provide feedback to the policy owner and appropriate business unit manager.

Exceptions: Any exception to the policy must be approved by the InfoSec team in advance.

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

Please review the following policies for acceptable use of JMT’s network and details on protecting information when accessing the JMT corporate network:

- Remote Access Policy
- Password Policy

7. Definitions and Terms

InfoSec Team: Stands for Information Security Team, which is comprised of individuals in the organization responsible for the definition, implementation, and monitoring of security policies and measures.