Information Technology Security Policy

Version Control

Version	Date	Description of Change
1.0	11-11-2025	Initial Release
1.1	05-01-2026	Integrated Access Control Policy into IT Security Policy
1.2	05-03-2026	Synthetic / AI-Generated Content Control under Prohibited Activities

Approval

Initiated By	Sagar Biswas & Kunal Naiya - IT Department
Department Approval	Soumen Roy - IT Department
Management Approval	Rajendra Mathur - CEO Sukalyan Sarkar - COO Rupayan Majumdar - CFO

Purpose

This policy establishes guidelines for secure and responsible use of Information Technology resources including but not limited to Internet and Intranet facilities at McNally Bharat Engineering Company Limited (hereinafter referred to as MBECL) to protect company information assets and ensure compliance with applicable regulations mentioned hereinunder.

Scope

This policy applies to all employees, contractors, consultants, and third parties using MBECL network resources, including all devices connected to the corporate network.

Internet Access Control

Internet access is provided strictly for legitimate business purposes. All traffic must pass through company-managed Firewall, Proxy, Anti-Phishing/Anti-Spam systems, and must be protected by Endpoint Protection Software. IT may restrict websites, bandwidth, or access based on business needs.

Acceptable Use

Internet usage must be business-related. Limited personal use, upon approval by concerned departmental head, may be permitted if it does not interfere with work, consume excessive bandwidth, or violate company policies.

Prohibited Activities

Accessing illegal or inappropriate content, downloading pirated software, installing unauthorized applications, bypassing security controls, spreading malware, or attempting unauthorized access to systems, although restricted, is strictly prohibited.

Creation, upload, download, storage, or dissemination of synthetic or AI-generated content, including but not limited to deepfakes, manipulated images, altered audio/video, or misleading digitally generated media, using company IT resources if such content is unlawful, misleading, defamatory, or detrimental to the organization.
All internet and email traffic passing through the corporate network shall be subject to security monitoring, filtering mechanisms, and threat detection systems implemented by the IT Department. Any suspicious, manipulated, or potentially harmful digital content identified through these controls must be immediately reported to the IT Department for investigation and appropriate action.

Email & Anti-Phishing Protection

All emails are filtered through Anti-Phishing/Anti-Spam security systems. However, users must exercise caution with attachments and links, and report suspected phishing attempts immediately to IT.

Downloading & Uploading Controls

Use of external USB storage device is strictly restricted unless permitted by management. Software downloads require prior IT approval. All downloaded files must be scanned by Endpoint Protection Software. Sensitive company data transmitted, if allowed by the management, over the Internet must be encrypted.

Website Blocking & Content Filtering

Web filtering mechanisms are implemented to block high-risk or inappropriate websites. Access to social media, unauthorized messaging applications or streaming services is restricted unless approved by Management.

Intranet / Internal Hosting Security

Intranet systems are accessible only within the corporate network or via secure VPN. Role-based access control must be implemented for internal documents.

Monitoring & Auditing

All network activity may be logged and monitored. MBECL reserves the right to audit usage to ensure compliance. Employees should not expect privacy when using company Internet resources.

Roles & Responsibilities

The IT Department is responsible for maintaining security systems and monitoring threats. Employees are responsible for safeguarding credentials and reporting incidents.

Password & Authentication Controls

Passwords shall be minimum eight (8) characters long including uppercase, lowercase, numeric, and special characters. Password history shall prevent reuse of last four passwords. Accounts shall lock after three unsuccessful attempts. Initial passwords must be changed upon first login. Passwords shall not be shared, written down, or transmitted in clear text.

Access Control

Access to business information and information systems shall be granted strictly on a 'need-to-know' and 'need-to-do' basis with written authorization from the concerned Department Head. Each User ID shall be unique and must not be shared. All access provisioning, modification, and revocation shall be performed by the IT Department. HR shall notify IT regarding new hires, transfers, role changes, and separations for necessary access updates.

Remote Access Control

Remote access shall be granted only to authorized users with formal approval. Access shall be through secure VPN with strong authentication mechanisms. Remote sessions shall be logged and monitored.

Physical Access Control

Data Centre, Server Room, and Communication Room shall be designated as Restricted Entry Areas. Access shall be limited to authorized personnel and protected through appropriate entry controls. Visitors shall be always escorted. Access rights shall be periodically reviewed.

Oracle eBusiness Suite Security

Access to Oracle eBusiness Suite shall follow role-based access control as ratified by concerned Head of Departments with Maker-Checker principles. User Responsibilities should be assigned depending on access privileges.

Data Protection, Backup & Patch Application

Database access shall be restricted to authorized IT personnel and monitored regularly. Complete back-up of Production instance in Oracle Cloud Infrastructure (IaaS) should be done daily unless requested by user for need-based contingencies. Application and database patching shall follow Oracle Critical Patch with concurrence of Oracle Support Service.

Incident Reporting

Any suspected security incident, malware infection, data breach or incidents in contrary to the policies mentioned in this document or seemed to be detrimental to MBECL's interest must be reported immediately to the IT Department.

Policy Assessment and Renewal

This policy will be reviewed annually or when significant technological policy changes occur.