BANK MANDIRI (EUROPE) LIMITED
POLICY STATEMENTS

VOLUME III

INFORMATION TECHNOLOGY

SECURITY POLICY

APRIL 2023

INFORMATION TECHNOLOGY SECURITY POLICY

1 Scope

This policy applies to all users of Bank Mandiri (Europe) Ltd (BMEL) computer-based information, including BMEL employees, temporary staff, board members, vendors, business partners, and contractors. The policy covers all IT environments operated by BMEL.

2 Purpose

The purpose of this policy is to manage information security within BMEL and maintain appropriate security controls in the information processing facilities within BMEL. Information is an important asset to BMEL, and it is BMEL's policy that such information must be protected from threats that may result in significant financial loss, reputational damage, or legal or regulatory violations.

3 Policy

3.1 Access Controls

3.1.1 General

All computer systems will have appropriate access controls. These controls will be defined for access to entire computer systems, specific data files, software applications, email, and other resources. Access controls can be specific to individual users or groups of users. Users will only be permitted access to those files and system resources they need to perform their job functions, only department heads can request this access. In a computer system environment, considerations will include:

a. Identification of the User to the computer system by Account Name and Password.

b. Access to required Files and Folders.

c. Account Restrictions.

d. Access to databases and associated Application software.

e. Other Privileges.

f. Template based access depending on the department on the Core Banking System (Flexcube).

3.1.2 Access Controls on User Accounts

Individual users will each be given a personal account for which they are responsible.

On the Core Banking System and Swift, separate templates are set up for each department, and access is granted based on these templates in the form of a user access matrix table. User access matrix tables are created to enforce the segregation of duties.

The user access is removed when a user leaves the bank (i.e., resigns, terminates, and/or mutations), and access to all systems and applications will be revoked for the user by IT. The process will be documented in the user access review report.

The user access matrix table on systems and applications will be reviewed once every 6 months by the compliance department to verify whether there are any changes regarding the user roles.

A user account will not be allowed to have more than one login session at a time.

3.1.3 Access to Files

User access to files will be granted according to individual or group needs. By default, access will be denied unless it is shown to be required.

Access to files containing confidential or sensitive information will be restricted. Only those users needing the information shall be given access to it, only department heads can request this access.

3.1.4 Access to Databases and their Associated Applications

There will be access controls on databases and associated software in line with current best practises as recommended by the relevant software vendors.

3.1.5 System Administration/Privileged Accounts

Sensitive system access for the privileged accounts on all systems will be restricted to system administrators and only used to install, configure, and maintain systems.

Privileged accounts are all-powerful profiles and must not be stored in procedures or policies or hardcoded into scripts or other code.

A copy of privileged accounts is help in the CEO safe in a signed sealed envelope.

3.2 Backup and Recovery

Backup forms an important component in improving operational resilience and recoverability. We follow a backup cycle that takes a backup to disc and securely uploads it to the Datto cloud.

Backup of servers and server files is automated and scheduled to run hourly from 8 a.m. to 6 p.m., Monday through Friday. These backups are stored on a Datto device located in the computer room, and the latest backup is securely uploaded to the Datto cloud daily over a managed line.

The backups are tested annually to ensure that BMEL's disaster recovery and business continuity obligations can be met.

All BMEL information and user files must be stored on the BMEL network. Users with PCs must ensure that BMEL information and user files are not stored on their PCs. The IT Department does not backup files held on PCs, so it is vital that users store files on the network to ensure backups are taken.

Users must not use cloud-based services for backups (Dropbox, Google, etc.) or for storage of BMEL information. It is also not permitted to use such services for the transfer of BMEL information between portable computing devices and the BMEL network. As the use of these services is considered a threat to confidentiality, their use with BMEL information is not permitted.

3.3 Data Confidentiality Considerations

3.3.1 General

Where data has been identified as personal, confidential, or sensitive, precautions will be taken to restrict access to the data to those individuals who need it to do their job.

BMEL information, including corporate, personal, confidential, or other sensitive information, will be stored only on the network in the appropriate shared folders.

Key points to consider:

a. It is every employee's responsibility to ensure that sensitive information at their disposal or in their possession remains secure.

b. Sensitive and Personal data must not be disclosed to other third parties without consent of the data owner unless there is a legislation or other legitimate reason to share information. (If in doubt, contact Compliance).

c. Do not discuss any sensitive information with other employees unless there is a clear business reason to do so.

d. Never leave documents or electronic media (including laptops, company phones, backup tapes etc) where they can be stolen or used without your knowledge.

e. Never leave sensitive information in a meeting room after use.

f. Delete any documents in laptops used for presentations.

g. As far as possible, Sign Off or shut your computer down when you leave your desk for long periods of time and at the end of the day.

h. Workstations should be locked when temporarily unattended. Auto lock is enabled for 15 minutes of inactivity.

i. Output containing personal, confidential, or sensitive information should be held securely (e.g., under lock and key).

j. Printouts containing personal, confidential, or sensitive information are treated as confidential waste when disposed of and are to be shredded instead of being thrown out as general waste.

k. Third party vendors who have access to customer data must be assessed and have appropriate data security controls in place. They should be assessed as part of the due diligence and approval process and reviewed regularly to ensure they continue to be compliant after the contracts are signed.

In order to conform with the Basic Principles of the Data Protection Act and to protect the confidentiality of client and personal data, the bank currently has a clear desk policy that must be adhered to. All correspondence worksheets and files relating to an individual or organisation must be stored in a locked filing cabinet. Staff were sent an email relating to this.

3.3.2 Safe Disposal of Equipment Used for Data Storage

All sensitive information is removed from hard drives on file servers by the IT Department before equipment is disposed of. Any IT equipment with storage being disposed of should be securely removed, and a certificate should be obtained from the vendor.

3.3.3 Data Sharing and Transfers

If there is no better option than email for the transmission of personal, confidential, or sensitive information, encryption should be used, and the message must be correctly addressed. The possibility of misaddressing could mean the information is delivered into the wrong hands, and it is the responsibility of the user to guard against such unwanted disclosures and comply with the Data Protection Act 1998 and GDPR.

The GDPR outlines six data protection principles you must comply with when processing personal data. These principles relate to:

a. **Lawfulness, fairness and transparency** – you must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.

b. **Purpose limitation** – you must only collect personal data for a specific, explicit and legitimate purpose. You must clearly state what this purpose is and only collect data for as long as necessary to complete that purpose.

c. **Data minimisation** – you must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.

d. **Accuracy** – you must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.

e. **Storage limitation** – you must delete personal data when you no longer need it. The timescales in most cases aren't set. They will depend on your business' circumstances and the reasons why you collect this data.

f. **Integrity and confidentiality** – you must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical measures.

3.3.4 Email

The bank provides electronic email to all employees who require it to carry out their business functions. All email messages are treated as work-related, and management reserves the right to monitor access and disclose the contents of user emails without the user's consent.

Email is to be used primarily for conducting the bank's business, and all messages composed, sent, received, and stored on these systems remain the property of the bank.

Employees must use their bank email for all business emails. Users are responsible for the content of all emails sent from their addresses.

Employees must not impersonate or try to impersonate another user's email identity for sending or receiving mail through the email system.

Employees should not forward any virus warnings of any kind to anyone other than the IT team. It does not matter if the virus warnings have come from an anti-virus vendor or have been confirmed by a reliable company or personal acquaintance. It is the responsibility of the IT Department and should not be acted on before receiving instructions.

Employees must not use the email system to distribute copyrighted material without appropriate authorization.

Employees must not use BMEL's email system to send unsolicited emails for personal purposes, private business activities, or personal amusement and entertainment.

Employees should be aware of the vulnerability of email messages to unauthorised interception, modification, and errors, as well as the possibility that they can be forwarded to third parties both within and outside the bank.

Phishing is an increasingly common type of fraud that can lead to the loss of personal information or a security breach in the bank's systems. A phishing attack is when a fraudster sends spoof emails that appear to come from a genuine website with the intention of obtaining your personal information.

a. Never respond to emails that request personal or financial information.

b. Never click on any links sent to you by email from an unknown person.

External Email

There are several risks associated with external emails, and these should be taken very seriously. Unsolicited emails should be treated carefully, particularly when sending or opening attachments, where users should always be aware of the risks of viruses and trojans.

Each incoming and outgoing external email is scanned for its size (maximum 50MB) and content according to rules and configurations that are set up within Microsoft Advanced Protection. The system monitors and manages all inbound and outbound external emails and may block messages that are classified as too large, spam, contain viruses or malware, or are possible phishing attempts.

BMEL's email domain uses DMARC, DKIM, and SPF to improve email security and deliverability.

If an email is quarantined for viruses, malware, or possible phishing attempts, a notification will be sent to the employee sending or receiving the mail to inform them. Employees can request the release of work-related emails that, for example, happen to be large in size. Requests should be sent to the IT department.

Although all emails are scanned, this does not guarantee that all viruses will be caught. If you receive a suspicious email from an unknown or unexpected sender, do not click on any links or attachments within the email. Delete the email and contact IT immediately, who will then advise on what you should or shouldn't do.

Users are not permitted to use cloud-based file storage or sharing services for the storage of BMEL information or for data transfers. Such systems and their security controls are outside the control of BMEL and can operate with security and data protection requirements that are not compatible with BMEL's own security and data protection requirements. As the use of these services is considered a threat to privacy and data confidentiality, their use with BMEL information is not permitted.

3.4 Network Management/Protection Controls

3.4.1 User Authorisation

BMEL will ensure that all computer system users are formally authorised to use the network by their department heads, HR, and the CEO.

3.4.2 Hardware Authorisation

Employees should not attempt to move IT equipment other than mobile devices.

All desktops and laptops are configured on a 'need to have' basis and are installed with the necessary applications required for a user to carry out their responsibilities. All users have now been issued laptops for home work. Sufficient care should be taken of the laptops to avoid theft or loss, especially on public transport. These laptops should not be left in a car overnight.

Any additional applications will be installed after approval from the relevant line manager and IT. The use of unlicensed software is prohibited.

It is illegal to make copies of software provided by the bank or distribute it to unauthorised persons. Software is issued by the bank for your use and is licenced to the bank and protected by copyright law.

Apart from IT staff, an employee does not have administrative rights on desktops or laptops.

Do not attempt to install or download any personal software or hardware onto the bank's network or equipment.

The IT department is responsible for setting up shared folders and restricting access to these folders to authorised users only.

IT will maintain an inventory of authorised network equipment, including network components, servers, and workstations.

3.4.3 Controls on Physical Access to Computer Equipment

Physical access to the servers and related components will be limited to authorised IT personnel.

The servers, backup facilities, UPS, network switches, etc. will be installed in locked areas that are only normally accessible to the IT department.

The computer room used to house the server and other sensitive system equipment will be kept locked at all times, and access to the room will be restricted and monitored.

3.4.4 Human Awareness of Security Issues

All users must agree to their responsibilities regarding security, use of computer system facilities, and use of information on the computer system. There will be IT security and cyber security awareness raised both through newsletters and e-learning sessions. The IT security policy will also be published with other policies and will need to be read by all staff. New staff will be provided with the policy.

Social Engineering: Breaches of information security often now involve criminals using psychological means to circumvent security measures as well as the use of technical measures. Large companies and individual internet users may be deceived into allowing criminals access to their computer systems, bypassing technical security defences. Such criminals' approaches by phone or in person may seem plausible and persuade the user to comply with their fraudulent requests. The victim, keen to appear helpful or intimidated by claims of authority or other pressures, may supply the criminal with the information needed to break into the system either on the spot or sometime later. If approaches are made electronically, the victim may receive a message persuading them to click on a link (a phishing attack), open an email attachment, or otherwise divulge information that they should not. Users need to be aware of the risks and wary of any unexpected approaches or occurrences. If you have any doubts about an email or any other approach, contact IT.

All users must be aware of these typical situations and exercise caution as described:

a. A computer becoming infected with a virus or trojan after its User has been tricked into clicking on a link in the hope of getting something for free.

b. Impersonation of authorised personnel with the intention of gaining access to restricted areas or to solicit information from staff.

c. Pretending to be IT/Support personnel for the purpose of soliciting account information.

d. Any fictitious tempting offer to solicit a response, thereby confirming a 'live' account which can be sold on to criminals who send 'spam' emails.

3.5 Physical Security

The physical security of the computer system, including servers and workstations, is a critical aspect of IT security.

To maintain protection against intrusions, it is important that access to critical computer system components (such as servers) be restricted to a small number of authorised individuals. Other considerations will include the protection of equipment against theft, fire, and electrical hazards.

The computer systems will be located in a locked room to which access is restricted to authorised IT staff.

Visitors to restricted areas should be supervised by authorised IT staff.

Employees leaving the bank should hand their access pass back to the IT Department, which has revoked or removed it.

3.6 Server Security Considerations

All use of a server will be prohibited unless the user has entered a valid user ID and password.

Backup systems will enable complete recovery of the Entre server operating system as well as data files in a timely manner.

Appropriate elements of hardware, such as disc mirroring, are installed on critical servers.

User-accessible servers shall have appropriate anti-virus protection running continuously and updated hourly.

3.7 System Hardening

The hardening of systems is critical to restricting unauthorised access and use. All desktops and servers are hardened to CIS Level 1, which includes but is not limited to the following:

a. Built-in Administrator account disabled.

b. Unused accounts removed or disabled.

c. Unused ports, services and protocols disabled.

d. No unnecessary software to be installed.

e. USB ports disabled.

f. Auto-lock after inactivity.

g. Anti-Virus/Malware tool installed.

3.8 Malware/Anti-Virus

All servers and desktops have Sophos Endpoint Advanced with Sophos Intercept X installed to protect them from all types of malware and malicious code.

BMEL has a process in place where the Sophos software is updated hourly, on access, and scheduled on demand. Suspicious files are quarantined, and IT is informed via email to investigate. All other incidents, such as failure to update, are monitored in Sophos Central, and IT is alerted.

A Cisco security appliance is also in place that has Advanced Malware Protection (AMP) enabled. Alerts are sent to IT.

3.9 Logs and Monitoring

The Cisco Meraki security appliance monitors packets flowing between the LAN and internet, between interfaces, and between VLANs through the SNORT intrusion detection engine. Any malicious traffic is automatically blocked, and an alert is sent to IT to investigate.

The logs on the Cisco security appliance are reviewed daily. The event logs on the Sophos Central manager are reviewed daily, and any unusual or suspicious activity is investigated by IT.

All logs are reviewed daily, and an entry is entered into the server log check list.

3.10 Regular Patching

Regular patching is critical to remedying any security vulnerabilities that exist in our technology. We follow a critical patching process whereby patches will be installed on a 7-day delay from release. This is for both servers and workstations.

A ‘0-day patch," or an emergency patch released by Microsoft, will be installed immediately and not wait for the 7-day delay.

3.11 Vulnerability Management and Penetration Testing

Vulnerability Management

The bank uses a vulnerability management tool that identifies any vulnerabilities and categorises them based on their criticality. A vulnerability assessment is carried out every 6 months, and advice from BMEL’s IT support (CITC) will be patched as quickly as possible.

Severity of vulnerability Assessment results refer to the following severity:

Severity	Description
Critical	CVSSv2 Score 10.0
High	CVSSv2 Score 7.0 - 9.9
Medium	CVSSv2 Score 4.0 - 6.9
Low	CVSSv2 Score 0. 1 - 3.9

Penetration Testing

Penetration testing is done annually for BMEL's external-facing interfaces. The test is carried out over the live and standby lines in the office. The test is carried out under "black box" conditions.

Vulnerability identified will be categorized into the following Risk Category:

Risk	Description
Critical risk	Critical risk vulnerabilities are those where an attack is highly likely and would seriously affect the confidentiality, integrity or availability of a system or sensitive information.
High risk	High risk vulnerabilities are those where the security of a system or sensitive information would be seriously affected but may require a more complex method or a highly skilled attacker.
Medium risk	Medium risk vulnerabilities are those where an attack forms part of a wider exploit, exposes less sensitive information or has other mitigating factors.
Low risk	Low risk vulnerabilities include non-critical information disclosure, more serious vulnerabilities that are very complex to execute and issues that have other mitigating factors.

Vulnerability and Penetration Testing results are reviewed and sent to the CEO, regardless of the severity of the findings. The CEO will decide whether the findings are accepted or need to be corrected. If the findings need to be corrected, the IT manager will propose an action plan and a timeline to the CEO.

Exception Mechanism

If the patches cannot be implemented as quickly as possible, referring to point (a) above regarding operational and/or system issues, the IT Manager shall proceed with the exception mechanism in a documented manner, containing the details of the vulnerability findings, a recommendation action based on the vulnerability scanning report, and the reason why the patches cannot be implemented. IT managers have to ensure that there is compensating control in place to compensate for the findings.

For the penetration testing findings that cannot be corrected, the IT manager shall proceed with the same exception mechanism in a document as mentioned above.

3.12 IT Equipment

The IT department is responsible for disposing of IT equipment. Where this is likely to have contained confidential data, the hard drive and tapes should be destroyed.

IT will use a certified third-party vendor to dispose of the bank's old equipment. A secure destruction certificate should be obtained and stored for all IT equipment disposal.

3.13 Internet Access

Internet access is restricted to authorised employees only. The bank reserves the right for authorised individuals to monitor internet usage at any time.

Employees can only access the bank's internet using their assigned user ID and password. Visitors will not be given internet access through this channel.

Internet access is controlled by Sophos Web Control and the Cisco Meraki Content Filtering system.

The use of modems is not allowed unless they are required for a particular purpose and have been authorised by the IT Department.

In certain cases, third-party personnel or other external users may be allowed access through the bank's Wi-Fi. The bank's Wi-Fi is completely independent and not connected to the bank's network in any way. The Wi-Fi password is changed periodically by IT.

Employees are not allowed to use the bank's computers to remotely connect to any non-bank computers other than those authorised by IT.

3.14 Information Security Incidents

Staff must report any security incident or information security concerns to IT. Examples of security incidents that should be reported are:

a. Network or workstation infected with a worm, virus, trojan or other malicious software.

b. Virus outbreak.

c. Phishing attack.

d. Data loss.

If you are unable to use your PC or any other particular system, this should be reported to IT.

3.15 User Identification and Authentication

User identification and authentication are the abilities to identify the user to the computer system and confirm the claimed identity of the user. The user identifies themselves to the computer system by entering a user or login ID, usually consisting of their name. The user's identity is authenticated when the user enters a valid password.

3.15.1 User Registration

The bank's IT systems will have user registration software for the creation of user IDs and the allocation of resources to them.

User profile monitoring or gaining access to another employee's email can be approved by the CEO after a request from the department head.

Users will be registered when the new user request has been received by the HR manager and approved by the CEO.

3.15.2 User IDs

Each user will only have one user ID, and the ID will be unique within the computer system.

Accounts known as 'guest' accounts are temporary accounts with specific access rights granted to authorised users, typically temporary staff, or contractors. At BMEL, the guest account has been disabled.

3.15.3 User Passwords

Individual users will each be given a personal account for which they are responsible. The account is for the sole use of the authorised user for access to BMEL's IT facilities.

The account must not be used by anyone else, and the password for the account must not be shared with any other person for any reason.

User passwords must be kept secret and should not be divulged or written down.

Password Guidelines

Employees should create passwords that are complex but easy to remember using the following guidelines:

a. Users should ensure that their passwords contain a mixture of different alphanumeric groups, lower case letters, upper case letters, symbols and digits.

b. Replace letters with numbers or characters.

c. The password associated with each profile must be kept strictly confidential.

d. The password must not be the same as the user ID.

e. Passwords should not contain personal data as these may be guessed easily.

f. Passwords should never be written down and should not be disclosed for any reason.

g. Users should be vigilant and avoid signing into the system when someone is looking over their shoulder.

h. Passwords must be changed immediately after certain events including, but not limited to:

- Suspected account compromise.
- Password expiry.
- Attempted or actual online fraud such as Phishing.

The user's supervisor, manager, or computer administrator does not need to know a user's password and will not ask for it.

Passwords will not be displayed on the user's screen when they are keyed in.

When a user forgets their password, the administrator will issue a temporary password. The computer system requires the user to change the administrator-assigned password as soon as they first log in.

The user will be able to change their own password without administrator intervention.

The user will be requested to follow good security practises in the selection and use of passwords.

If suspicion arises that a password may be known to an unauthorised party, the password should always be changed immediately and without regard to whether a regular password change is due.

These are our password policies for the main systems:

System	Attributes	Expiration	Other
Computer Sign on Password (Active Directory)	Minimum 8 characters, capital letter, number and special character	90 days	5 attempts allowed
Flexcube (Core banking system)	Minimum 8 characters, capital letter, number and special character	90 days	5 attempts allowed
Swift (Total Messaging)	Minimum 8 characters, capital letter, number and special character, MFA	90 days	5 attempts allowed
Remote Working via Logmein	Minimum 7 characters, capital letter, number MFA	90 days	3 attempts allowed

The user will be required by the computer system to choose a different password from previously used passwords.

Where technically possible, the user will not be able to use expired passwords as the new password when the system forces a password change.

IT is responsible for ensuring the password policy is effectively maintained and followed.

3.16 SSL Certificates

BMEL uses an SSL certificate issued by Starfield Technologies via 123-Reg, and the SWIFT service bureau certificate is issued to BMEL by Finastra.

The validation of the SSL certificate will be monitored and reviewed regularly, at least once a year.

The general requirements for the SSL encryption process can be listed as follows:

a. Using Secure File Transfer Protocol (SFTP) mechanisms in accessing, transferring, and managing files on data streams.

b. Encrypt electronic data with at least 256-bit Advanced Encryption Standard (AES) or Data Encryption Standard (3DES).

c. Encrypt communication media with at least Transport Layer Security (TLS) 1.2 and a minimum of 2048-bit private keys.

4 Storage of Corporate/Customer Information

All BMEL information must be stored on the network storage provided.

USB memory sticks and external hard drives **must not** be used to hold any BMEL information, including personal data, corporate confidential information, or otherwise sensitive information.

Corporate documents and files should be stored in the appropriate shared folders, not in email systems.

BMEL information must not be stored off-site.

4.1.1 Remote Working

4.1.1.1 Mobile Computing

Portable computing devices are frequently lost or stolen. Loss or theft of a device could result in a costly breach of information if adequate protection has not been applied. This policy describes protection measures aimed at mitigating the effects of such a loss. However, the user is reminded that it is their primary responsibility to take care of the device and minimise loss or theft. They should not be left overnight in vehicles.

Portable computing devices must not be used for the permanent storage of any kind of information. Any copy of such information held on the device must only be temporary and must be erased after use. Emails should not be used for sensitive information, as they are particularly vulnerable on portable devices and are often difficult to decrypt. Ensure sensitive emails are not used or retained at all on these devices. All laptops that have been issued to the users are encrypted using BitLocker.

For mobile devices such as smartphones, the user **must** ensure the device PIN or password has been set and that the device is set to automatically lock after a period of inactivity. This will help protect the device against misuse and is an extra safeguard for personal contact details or any other confidential information held on the device, should it fall into the wrong hands. The user is reminded that any device without a PIN or password **must not** be used to hold any BMEL information or confidential details.

The user is responsible for physically safeguarding the equipment against unauthorised access, misuse, theft, or loss.

The user of the equipment must comply with the security requirements of this document at all times.

The use of USB devices on laptops is not permitted, and USB access has been disabled.

4.1.1.2 Working from Home

The bank has now made available remote working capability, which now forms part of our resilience monitoring to ensure this facility is available at all times. When working from home, users needing to work with BMEL information should use the remote access provided by the BMEL laptop to access it. Other than this method, BMEL information must not be carried in any other media.

The bank's current IT infrastructure does not support "bring your own device' (BYOD), and the only option to access BMEL information securely is through the approved process using the bank's laptops.

The user is responsible for safeguarding the equipment against unauthorised access. Misuse, theft, or loss.

The user is responsible for ensuring that, where the equipment might be used by others (family members), no BMEL information is left open to breaches of corporate or personal privacy and that the equipment is not left in circumstances where other breaches of security may occur. The same safe practises (e.g., locking screens when not in use) should be followed while working from home.

The user must ensure that, where possible, reasonable protection measures are in place and operating where applicable, i.e.:

a. Firewall.

b. Anti-virus software is updating automatically.

c. Up to date security patches are installed for both operating systems and applications. Doing so will help protect the laptops against security vulnerabilities that have been identified.

d. Home wireless networks must be properly secured against eavesdropping and intrusion.

If any users have any doubts about the above points, the IT department must be notified.

The user of the equipment must comply with the security requirements of this document at all times.

The network storage provided must be used for the storage of BMEL information and must only be accessed by one of the currently approved methods. The laptop itself must not be used as storage for any BMEL information.

Remote access permitted over the internet is encrypted and authenticated. Authorised users will have a remote access password and secret over and above the normal password that is used when logging into the office. The bank has also implemented dual-factor authentication, which ensures that any access is authorised subject to a code entered and sent to their mobile device.

There is no connection to the bank's network from outside the bank other than via the secure LogMeIn system in place.

4.1.2 Third Party Access Control

Physical access for third parties and contractors will be granted after the necessary approvals are in place. Once access is agreed upon, user access is restricted to the systems and information that are required.

All third parties must sign Non-Disclosure Agreements (NDAs) with the bank before accessing information systems.

BMEL uses LogMeIn, whereby monitored access can be given to third parties. This is a secure connection, and their activity is monitored during their access.

4.1.3 Software

Copyrighted and licenced software may not be copied or distributed by users in contravention of the licencing agreement.

It is not permitted to operate corporate workstations in an experimental manner. For example, by trialling software installed on a removable disc and/or modifying elements of the operating system manually or by application download (screen savers, etc.),

Personal use of peer-to-peer networking and file-sharing applications is not permitted on any of BMEL's systems.

Concerns over this type of software include:

a. Peer-to-peer software requires an agreement from the end user to provide services to the peer-to-peer network using BMEL's resources. Individual users are not empowered to provide such content.

b. Increased risk of virus infection over peer-to-peer networks.

c. Spyware and other privacy risks as far as full access to the computer's hard drive.

d. Legal risk due to storage of copyrighted material Peer-to-peer software may store such material without the knowledge of the workstation user.