Metro Bank (UK) PLC

Acceptable Use Minimum Standard (AUMS)

Appendix 2 to MBPOL48

V. 1.6

Document Summary

Document Title	Acceptable Use Minimum Standard (AUMS)	
Document Version	1.6	
Date of Current Version	09/11/2021	
Document Status	Final	
Document Classification	INTERNAL	
Owner	Chief Information Security Officer (CISO)	
Peer Reviewed by	Richard Norman, Julia Babahina	
Approved by	Name	John Skipper
	Date	09/11/2021

Version control

Date	Version	Author	Description
27/6/2017	0.1	Arkam Usair	Supersedes Acceptable Use Policy v2.0(Retired)
28/6/2017	0.2	Arkam Usair	Peer Review by Timothy Harris.
30/6/2017	0.3	Arkam Usair	Peer Review by Mark Avery
5/7/2017	0.4	Arkam Usair	Minor amendments based on HR Feedback
12/7/2017	0.5	Arkam Usair	Review by William Iuliano for Metro touch
18/7/2017	0.6	Arkam Usair	Review by a Sample of 5 Junior Colleagues
28/9/2017	0.7	Chris King	Approval
29/9/2017	1.0	Martyn Atkinson	Approval

Date	Version	Author	Description
22/10/2019	1.1	Carole Embling	Annual review with minor changes
04/11/2019	1.2	Carole Embling	Amendment to 1.4 and ability to capture of 3rd party acceptance signatures
21/02/2020	1.3	Waqas Javed	This document has been raised from Tier 3 to a Tier 2 standard. This issue includes a revision of existing content and where required further content and sections has been added new. Alignment with ISO 27001 standard.
08/09/2020	1.4	Carole Embling	Added reference to MFA More direction regarding printing
	1.5	Carole Embling	Minor Change: Direction provided on the removal of assets from MB premises.
09/11/2021	1.6	Julia Babahina, Richard Norman	Annual review with minor changes. Updates to structure and organisation of the document in light of the updated Policy Governance Framework v. 2.0

Table of contents

1 Introduction

Metro Bank PLC is committed to preserving the confidentiality, integrity, and availability of all information assets throughout the organisation. This is to preserve the bank's competitiveness, profitability, and reputation, and to ensure continued legal, regulatory, and contractual compliance.

The Acceptable Use Minimum Standard (AUMS), which supports the Metro Bank Information Security Policy, mandates the acceptable minimum standards expected of Metro Bank Colleagues or other users requiring access to Metro Bank information assets and systems.

Note: all users must read and sign the AUMS at least annually. Paper copies and physical signatures must be used where the user does not have access to do this on MBU.

This AUMS is consistent with, and promotes, Metro Bank core values, which are as follows:

a) **Integrity is Our Passion:** We are committed to honesty and integrity in all facets of our business.

b) **Respect and Professionalism are Our Hallmarks:** We treat our customers and staff with respect and deliver professionalism in every interaction.

c) **We Embrace Diversity:** We value the various beliefs, cultures, and experiences of our customers, our employees, our shareholders, and our community.

d) **We Deliver Unparalleled Service with a Personal Touch:** We value direct interactions with our customers and are committed to excellent customer service.

e) **We Do the Right Thing:** Our unique approach to decision-making includes the diverse opinions, skills, and experiences of our team to ensure that we do the right thing–every time.

f) **We Promote Employee Growth and Development:** We invest in human potential and develop employee talent. Our customers can count on the competency and capacity of our team.

g) **We Care About Our Employees:** We encourage and promote a healthy work/life balance for our employees. We provide affordable benefits and a relaxed working environment.

h) **We Play by the Rules:** We have a strong compliance culture and strive to exceed industry performance standards.

To achieve our core values, Metro Bank is committed to protecting our customers, colleagues, and Metro Bank from illegal or damaging actions by individuals, either intentional or unintentional.

Effective security is a Bank-wide effort requiring the participation and support of all Metro Bank Colleagues, Contractors and Consultants who have access to Metro Bank information assets and information system(s).

1.1 Purpose and scope

This Minimum Standard applies to all Metro Bank colleagues, temporary colleagues, business users, suppliers, contractors, service providers and business partners (hereafter referred to as "users") in all business areas and outsourced services that use and manage our information and information assets to support the delivery of Metro Bank's business regardless of location.

This document and the associated logical, technical, and physical controls referred to within it are the minimum mandatory requirements for Metro Bank.

Inappropriate use of Bank's information and information assets exposes Metro Bank to the risk of:

a) security breaches

b) compromised network systems and services

c) civil penalties and judgements

d) non-compliance with regulatory requirements.

The implementation of this standard contributes to the mitigation of these risks.

1.2 Framework, policy, and ownership

This Minimum Standard is governed by the Operational Risk Framework and associated Information Security Policy and supports the Information Security Management System (ISMS). The CISO is the owner of this Minimum Standard.

1.3 Associated policies and standards

Below is the list of Metro Bank's Policies, Minimum Standards and documents that should be used in conjunction with this Minimum Standard.

Reference	Title
MBPOL48	Information Security Policy
Appendix 1 to MBPOL48	Asset Management Minimum Standard
Appendix 3 to MBPOL48	Access Control Minimum Standard
Appendix 4 to MBPOL48	Colleague Security Minimum Standard
Appendix 9 to MBPOL48	Physical and Environmental Security Minimum Standard
Appendix 13 to MBPOL48	Information Classification and Handling Minimum Standard
MBPOL61	Data Protection Policy
MBPOL57	Records Management Policy
Metropedia	Metro Bank Social Media Guidelines
Metropedia	Records Retention Schedule

1.4 Summary of roles and responsibilities

The table below provides a summary of roles and responsibilities associated with this Minimum Standard.

Roles Responsibilities	Users	Third parties	CISO Team	Data Protection	CISO	IPRF
1) Be aware of, and comply with, this Minimum Standard and the requirements it lays out	R/A	R/A				
2) Acknowledge understanding of the obligations described within and agree to follow them	R/A	R/A				
3) Use Metro Bank’s information assets and information systems only for business purposes and for limited personal use in line with Metro Bank’s Information Classification and Handling Minimum Standard	R/A	R/A				
4) Not attempt to bypass any security controls	R/A	R/A				
5) Complete training on their data privacy and information security obligations on induction and as part on the mandatory training programme	R/A	R/A				
6) Report detected or suspected privacy and information security incidents, concerns, and events	R/A	R/A				
7) Provide advice and support on handling information assets (including personal data)			R/A	R/A	I	I
8) Provide advice and support on information security-related matters			R/A		C/I	I
9) Update this Minimum Standard on annual basis or as required to accommodate changed circumstances	I	I	R	C	A	I
10) Approve exceptions to this minimum standard			C	C	R/A	I
11) Monitor compliance with this minimum standard			R		A	I
12) Manage risks associated with acceptable use of information assets	R	R	R		A	I
13) Provide training and awareness associated with this Minimum Standard			R	C	A	I

R (Responsible) – the person who is assigned to do the work

A (Accountable) – the person who makes the final decision and has the ultimate ownership

C (Consulted) – the person who must be consulted before a decision or action is taken

I (Informed) – the person who must be informed that a decision or action has been taken

1.5 Privacy

Metro Bank respects the rights of its colleagues to privacy. Under the terms of the Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356), Metro Bank reserves the qualified right to monitor usage of its communication and technology services and to intercept communications, including telephone calls, web browsing, email transmissions, and other communications by colleagues in order to maintain the services, comply with regulations, and to investigate or detect unauthorised or inappropriate use of our systems and equipment.

All Metro Bank's business information assets are routinely monitored and logs that record activity are maintained for legal, regulatory & compliance and system maintenance purposes.

Inevitably personal communications may be recorded and monitored as part of this process. Metro Bank will act reasonably to ensure that colleagues' privacy is not affected.

2 Information assets and information systems

Principle: users must use Metro Bank information assets and information systems only for business purposes and for limited personal use and ensure that they are handled securely with required protections.

Both Information assets and information systems have value to Metro Bank, and therefore present a monetary, reputational, operational, or regulatory risk.

Note: Users must use Metro Bank information assets in accordance with the Asset Management Minimum Standard and the Information Classification and Handling Minimum Standard.

2.1 Unacceptable use

Metro Bank's information assets must not be used in any way that is:

a) illegal

b) abusive

c) offensive or obscene, including by accessing, viewing, or distribution of:

- pornographic images or material
- other images, text or materials that are offensive or discriminatory, including those that discriminate based on race, ethnicity, nationality, religion, religious beliefs (and other beliefs), political opinions and views, age, disability, marital status, gender, or sexual orientation

d) threatening

e) defamatory

f) financially or commercially detrimental to Metro Bank

g) in breach of licensing or copyright requirements

h) unethical or

i) excessive.

In addition, users must not identify themselves as another individual, or as representing any other organisation, in any way.

2.2 Limited personal use

By choosing to use Metro Bank information assets for limited personal use, users accept that their communication and web browsing activities might be monitored.

When using Metro Bank information assets users must:

a) not knowingly introduce a computer virus or other harmful software to Metro Bank information system

b) not knowingly circumvent Metro Bank security controls including the installation or use of VPNs, anonymous proxies or any other tools or devices that have not been authorised by the Bank

c) not access copyrighted material (e.g., streaming video or broadcasts) except through approved formal channels

d) not use encryption for anything other than authorised business purposes

e) not use any Metro Bank information classified as INTERNAL, RESTRICTED or CONFIDENTIAL for personal use

f) not use personal accounts for Metro Bank business. This includes Metro Bank business related communication, sending or receiving business related attachments, and / or emails containing Metro Bank information

g) not use Metro Bank accounts for personal use

h) not allow personal use to interfere with their normal duties

i) not engage in activities for financial profit

j) not adversely affect the safety, health or wellbeing of themselves and others

k) not cause regulatory or reputational damage to Metro Bank and

l) not adversely affect Metro Bank financially.

Metro Bank accepts no responsibility for issues arising from the personal use of Metro Bank's information systems, which is undertaken at the user's own risk.

2.3 Handling of information

Users must exercise care when handling (e.g., creation, use, copy, sharing, storage, destruction, and retention) Metro Bank information. If in doubt, all information must be treated as INTERNAL (unless otherwise classified).

Extra care must be exercised when handling CONFIDENTIAL information. These additional requirements include and are not limited to the following.

CONFIDENTIAL information:

a) must not be accessed or modified without appropriate permission and authority (usually with the permission of Information Owner)

b) must be kept locked away and can only be used in designated areas approved by Information Owner

c) must always be encrypted, including when shared electronically

d) must be disposed of in confidential waste bins only (note: general waste bins must not be used for disposal of business information regardless of classification)

e) must only be accessed and used in suitably secure environments.

Note: users must refer to the Metro Bank Information Classification and Handling Minimum Standard for more details on how to classify and handle different types of information.

2.4 Corporate devices and equipment

When corporate devices and equipment are used for accessing Metro Bank information assets users must:

a) not, nor attempt to, bypass, tamper with or remove any security configuration such as authentication mechanisms and access controls

b) not move or remove any corporate devices and equipment from Metro Bank premises without prior approval from Line Management and the AMAZEING Support Helpdesk except where assets have been specifically assigned to them such as laptops, mobile phones

c) not, or attempt to, use VPNs or other methods that mask the logical and / or physical location of the equipment and the user

d) lock any logged-on device when not in use or out of the direct control of the user

e) store unattended devices securely, both on-site and off-site

f) inform Metro Bank when the device or equipment is no longer required

g) not share the device with others unless supervised by the owner

h) inform the Metro Bank AMAZEING Support Helpdesk immediately upon loss, theft, or misuse of device

i) must not use any corporate devices and equipment to communicate with, or conduct any bank business with, anyone located in High-Risk countries

j) not use authorised BYOD devices to conduct any bank business with anyone located in High-Risk countries

Note: See the High-Risk Country Bump Up Table on Metropedia.

Users must not assume the ownership of corporate devices and equipment provided to them by Metro Bank. The ownership of corporate devices and equipment is retained by Metro Bank.

2.5 Non-Metro Bank devices and equipment

When accessing Metro Bank information assets and information systems from non-Metro Bank devices and equipment, the requirements for using corporate devices and equipment remain applicable, and users additionally must not:

a) configure any additional devices for use with Metro Bank information assets without Bank's approval; and

b) hold or access any non-PUBLIC Metro Bank information on non-Metro Bank devices unless the user has explicit approval (e.g., BYOD).

Third parties (e.g., contractors, consultants, and service providers) must not use non-Metro Bank devices when carrying out work on behalf of Metro Bank without prior approval from the Information Owner and the CISO, or his nominated delegate.

3 Return of information assets

Principle: all users must return all Metro Bank's assets in their possession upon termination of their employment, contract, or agreement, or when instructed.

When users no longer provide services to Metro Bank, they must return all physical and electronic Metro Bank assets that have been issued to them, which include hardware, media storage devices, physical and logical access tokens, Metro Bank documentation, software, and identity badges. Users must not transfer any Metro Bank information to non-Metro Bank devices under any circumstances.

In all cases where authorisation has been granted to process Metro Bank information on non-Metro Bank devices, all relevant information must be securely transferred to Metro Bank and/or securely destroyed as agreed in advance with Metro Bank.

In cases where user has knowledge that is important to ongoing Metro Bank operations, that information must be documented and transferred to Metro Bank.

4 Information ownership

Metro Bank's information remains the property of Metro Bank regardless of where it is processed or stored.

5 Passwords and user authentication

Principle: users must authenticate themselves by using their unique username and password as login credentials and ensure that they use and handle them securely. Where provided, MFA must be used to supplement system security.

Users must keep their passwords private by:

a) not sharing them and

b) not recording them where others can access them.

Users are accountable for any actions or activities they carry out on any Metro Bank information system(s).

Users must choose strong passwords or passphrases (minimum eight-character length, mixture of numbers, upper/lower case and special characters, non-dictionary-based words or use three or more words with other characters) in order to help prevent someone from guessing their credentials.

Note: further guidance can be found in Access Control Minimum Standard.

5.1 Allocation of passwords

Users can reset their Windows / email account password or unlock their account using the Microsoft Self-Service Password reset (SSPR). Users requiring a password reset for other systems must contact the Metro Bank AMAZEING Support Helpdesk.

Users utilising Microsoft Authenticator application for MFA will be automatically registered to SSPR. Whereas users utilising hard tokens will have to manually register for SSPR in their Microsoft account “Security Information” section by choosing between authenticating with either security questions or with alternative email address.

If a user suspects that their or another colleague’s password has been compromised, they must report this to their Line Manager, Operations Security or AMAZEING Support Helpdesk.

Users requesting new passwords or password changes will be required to verify their identity before a password can be issued and / or before user access controls are reset or unlocked.

For high-risk accounts (e.g., administrator accounts, payment accounts or accounts that have access to personal data or CONFIDENTIAL information), requests might undergo additional verification.

5.2 Protecting passwords

Users are accountable for any actions or activities carried out on any Metro Bank information system using their account.

Users must always keep their passwords secret. Passwords must NEVER be shared with anyone – including with IT Support or anyone else.

Users must not:

a) enter their password where they can be overlooked

b) store passwords in a file on a computer system or mobile device (e.g., phone or tablet etc.) without encryption

c) use the ‘Remember Password’ feature of application e.g., web browsers

d) use the same password for different corporate accounts, nor use the same password for corporate accounts as for their other personal accounts (e.g., Yahoo, Facebook)

e) rotate through a list of favourite passwords - passwords should be changed entirely

f) contain their username in their passwords and

g) use single dictionary words within their password (e.g., Metro, Amaze, Amazing) and commonly used derivatives (e.g., M3tr0).

5.3 Password good practice recommendations

To make it easier to set and use good passwords, users must:

a) consider using passphrases instead of passwords for example, ‘***I love my children***’ becomes ***1Lovemychidr3n!***, which is both easily remembered and strong as it contains upper and lower case letters, numbers and a special character (the exclamation mark)

b) consider using longer passwords than required as password strength typically increases significantly with length

c) not use words easily associated with themselves (e.g., pet names, favourite sports team, car make or similar)

d) not use seasonal or topical words (e.g., Easter, Christmas).

6 Email

Principle: all users must use Metro Bank email system only for business purposes as part of their role.

Users are responsible for all email activity within their email account, including storage of emails, sending of attachments and any automatically generated emails such as out of office notifications.

Users must not:

a) send emails in another person's name without their express written approval/instruction

b) send sensitive customer details (e.g., credit card numbers, passwords, account details) unless encrypted

c) send any emails to personal email addresses, unless in direct support of business need. For avoidance of doubt the sending of any emails to your personal email address from your Metro Bank account is not permitted

d) auto-forward emails to any non-Metro Bank (metrobank.plc.uk) email accounts without explicit prior written approval and

e) access or attempt to access any email account that is not in their own name, unless granted access to do so by the email account owner or where access is requested, authorised and granted via the AMAZEING Support Helpdesk.

All emails are logged and monitored and can be retrieved when required.

Metro Bank reserves the right to withdraw or restrict access to the email system at any time.

Metro Bank applies automated controls to limit unacceptable emails reaching users from outside of Metro Bank. As these controls cannot be 100% effective, users must report suspicious, harmful or emails containing undesirable content (as listed in section 2.1 Unacceptable Use) to allow Metro Bank to improve the automated filters.

6.1 Receipt of inappropriate email

If users receive an email that is harmful or contains undesirable content (as listed in section 2.1 Unacceptable Use) they must:

a) not reply to the sender

b) not delete the email

c) not forward the email and

d) inform the People Team and seek advice from their Line Manager.

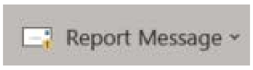
6.2 Spam and phishing emails

Metro Bank has controls in place to block spam and phishing emails however users might still receive unwanted emails.

When users receive spam or phishing emails they must:

a) not reply to the email as replying confirms your details which can result in receipt of additional spam emails

b) not click on any links within a suspected spam or phishing email and

c) use the Report Message  button in Outlook. Where this is not possible, users must add the suspect email as an attachment to a new email and send that to the *Internal Phishing* mailbox (internalphishing@metrobank.plc.uk).

7 Internet

Principle: Internet access is provided primarily for business uses. Users are permitted a reasonable degree of personal use, providing that it is not excessive, does not cause performance issues for the Bank and does not interfere with their day-to-day work.

Where possible, Metro Bank does block illegal and obscene websites but unfortunately, due to the nature of the internet, users may still be at risk of encountering sites containing offensive, libellous, unlawful, or abusive material. In these cases, users must exit these sites immediately and report it to their Line Managers, and AMAZEING Support Helpdesk. Metro Bank will take action to attempt to reduce further occurrences when informed by a colleague of unacceptable content still being available.

It is the responsibility of users, when downloading any content from the internet, to verify that it is virus free, that they and Metro Bank have a legal right to download it and that is not subject to any national or international restrictions.

Users must not download any software, such as games, freeware, shareware, evaluation software, fonts, music, or other media that is protected by copyright, onto Metro Bank computers and systems.

Streaming audio or video can impact the performance of the Metro Bank network so should only be used for legitimate business purposes. For avoidance of doubt, use of Metro Bank equipment and networks to stream online services such as sports, television, or music, is not permitted.

Metro Bank reserves the right to restrict access to any internet-based service that might pose a risk to information security, or to withdraw these services from any colleague at any time. All requests to access restricted websites require approval by the CISO team.

Note: users must use the Metro Bank internet in accordance with Section 2 (Information assets and Information Systems).

8 Social media

Principle: users accessing social media services and social media networking websites must ensure that the use is appropriate, is not excessive, does not cause performance issues for the Bank and does not interfere with their day-to-day work.

The use of social media comes with a responsibility for appropriate use. Whilst Metro Bank prides itself on being an open and transparent Bank, it is important to protect the sensitive and CONFIDENTIAL information of Metro Bank, our colleagues, customers, and suppliers, and to ensure the Metro Bank brand is represented in the right way.

8.1 Yammer

Metro Bank has supplied colleagues with an internal social media application called ‘Yammer’. Users are encouraged to participate in dialogue on Yammer and to use it for internal knowledge sharing, customer success stories, praising colleagues etc. However, Yammer should not be used for 1:1 conversation with other colleagues and sensitive data must not be included in Yammer posts.

8.2 Personal social media accounts

Users must ensure it is made clear that their personal social media account does not represent Metro Bank’s views and opinions.

Users should be aware of mixing personal and professional life in the social media world as these can easily intersect. Metro Bank respects the right of colleagues to speak freely, but you must remember that other employees, customers and suppliers often have access to the online content you post. Keep this in mind when publishing information online that can be seen by more than friends and family as it can be reposted in an unrestricted environment on other social media. Social media never forgets, once published it is essentially a permanent record.

The use of personal social media accounts to exchange or convey information about Bank’s operations, its clients/customers or any information about technologies used is strictly prohibited unless approved by Metro Bank.

Users must not:

a) post any personal information, including special category data, related to our employees, customers, and suppliers unless it is in line with the established lawful basis

b) post any non-PUBLIC information about Metro Bank or its systems without prior written consent

c) create or transmit material that might be defamatory or incur liability for Metro Bank

d) post messages, images, links to material or content that is inappropriate

e) respond to customer, third party or customer service-related comments on Metro Bank’s social media channels (note: these will be responded by Amaze Direct or the Social Media team)

f) publish or share any copyrighted software, media or any materials owned by third parties, unless permitted by the third party

g) share links to illegal copies of music, films, games, or any other software.

Users must:

a) be vigilant when using social media and watch for phishing scams, where scammers may attempt to use deception to obtain information relation to either Metro Bank or its customers and

b) avoid clicking on links in posts, updates and direct messages that look suspicious

c) where necessary reset privacy settings on their social media accounts so that their personal information is visible only to those users who they are willing to share it with.

Users must interact only with Metro Bank's official social media handles, which are as following:

a) Facebook: https://facebook.com/MetroBankUK

b) LinkedIn: https://www.linkedin.com/company/metro-bank-uk-/

c) Twitter: @metro_bank and @metrobank_help

d) Instagram: @metro_bank

Users can "like" and post comments on Metro Bank's official social media channels as themselves and share official Metro Bank posts to their personal social media channels in line with the guidelines provided in this section.

Users must not react or respond to negative posts or to a third party's attempt to start a negative conversation about Metro Bank. If you see someone post a question to the @Metro_Bank or @MetroBank_Help handle, we ask that you leave this to be handled by Amaze Direct's Twitter team (@MetroBank_Help). If any queries are directed to you directly on Twitter, or you see someone ask a question to /about Metro Bank, but they haven't tagged the @Metro_Bank or @MetroBank_Help handle, please pass them onto @MetroBank_Help. If they ask a question on any other social channel, you can share our Amaze Direct number: 0345 0808 500, or 0044 203 402 8312 if they are abroad.

Note: all users must follow Metro Bank Social Media Guidelines when using social media.

8.3 Metro Bank social media accounts

'Official' Metro Bank social media accounts are Information Assets and represent significant risk to Metro Bank if not used and managed appropriately. Anyone using a Metro Bank Social Media account must do so only for business purposes and the account must be managed in accordance with the Information Security Minimum Standards. User authentication and access controls including MFA (where technically feasible) are critical controls on these services and anyone using them must apply the same diligence when using these services as they do with their Metro Bank Windows account.

9 Fixed telephone systems

Principle: all users must use fixed telephone systems only for business use.

Users must not divert telephones to external or personal telephones, unless authorised by their Line Manager.

Metro Bank reserves the right to record and monitor telephone calls made through its telephony infrastructure.

10 Voicemail

Principle: when users are issued with a voicemail account, they must handle it securely and ensure that it is protected.

Users must:

a) protect voicemail accounts by using pin numbers and

b) change the default pin number to a personal code.

11 Removable media

Principle: the use of removable media is restricted and only approved, upon request, for business purposes. When using removable media, users must use it securely and apply appropriate protection to information that is stored or processed on it.

Use of removable media is not generally permitted and will only be allowed in exceptional circumstances and for temporary storage during transport of data. When using removable media for the storage and transport of Metro Bank information, colleagues must:

a) only use Metro Bank approved removable media

b) only use removable media as a temporary option to store and transfer information. Once the transfer has been made, the information shall be securely destroyed (contact Amazeing Support or the Security Operations team for guidance)

c) encrypt any Metro Bank information not classified as ‘Public’ in accordance with the Information Classification Minimum Standard

d) not transfer any Metro Bank information not classified as ‘Public’ (in accordance with the Information Classification Minimum Standard) from any removable media devices to any external device in unencrypted form unless expressly approved by the CISO or authorised delegate

e) only use removable media in conjunction with systems that have anti-malware protection

f) not share details of encryption passwords or pin codes for removable media unless authorised by the Information Owner for information sharing purposes

g) store removable media in a secure location e.g., locked drawer and / or cabinet when left unattended

h) not share removable media containing Metro Bank’s information with others, unless instructed by the Information Owner

i) regularly review the contents of removable media to identify out of date or unwanted files and

j) securely destroy unwanted files when no longer needed.

12 Software

Principle: all users must use only authorised software and as mandated by Metro Bank.

All software required to maintain and run the Metro Bank workstations and mobile devices are installed on these devices and must not be altered. Users must not install additional software onto any Metro Bank device except from the approved Metro Bank Software Centre or run additional software from any form of removable media, or the internet. Installation of any unauthorised or unlicensed software on the Metro Bank workstations and mobile devices is prohibited.

Metro Bank does not support non-standard system configurations and reserves the right to remove such systems from the network and undertake any necessary incident management or root cause activities necessary, should they pose a security risk to Metro Bank.

Users must not install patches and service packs on their workstations and devices unless directed/instructed by the AMAZEING Support Helpdesk.

Where additional software is required, users must direct their request to the Metro Bank AMAZEING Support Helpdesk, approval will be required by their Line Managers and appropriate SMEs within the CIO function (to ensure that the new software complies with all technical standards and does not cause security or performance problems).

13 Printers and photocopiers

Principle: all users must use and securely handle Metro Bank authorised printers and photocopiers and the associated physical media.

Users must:

a) not connect Metro Bank laptops to non-Metro Bank approved printers without prior approval from the CISO team

b) not print any Metro Bank documentation unless the printer is managed by Metro Bank and is in Metro Bank premises (or the user has applied for, and been granted, permission to print in that location)

c) not print, scan or photocopy sensitive or CONFIDENTIAL information without the prior authorisation of the Information Owner unless doing so is specifically required by the colleague's role

d) use 'Secure Print' when printing sensitive documents (if available) and collect the output as soon as practicable after printing, where the 'Secure Print' function is not available output must be collected immediately

e) not allow output to remain unattended at the printer for any length of time after printing, scanning, or copying

f) securely dispose of any unwanted documents containing Metro Bank information in the confidential waste bins provided

g) notify IT desktop support team if a printer or photocopier jams or malfunctions in the process of processing sensitive information so that any such material can be recovered / destroyed before retrying

h) notify Operations Security team, Reception colleagues (for Amaze Central), Site Managers (for Amaze Direct) or Store Manager (for stores), if any information is found unattended on a printer or copier

i) not copy material protected under copyright law or make that material available to others for copying, unless permitted to do so under licence or written agreement.

14 Postal system and couriers

Principle: when transferring Metro Bank information assets using postal system and / or couriers, all users must apply appropriate protections to preserve its confidentiality, integrity, and availability.

Users must:

a) where possible, deliver sensitive data to its recipient by hand (personally or through an authorised nominated person), alternatively, such information must be sent by a reputable provider and an audit must be retained of the successful delivery

b) ensure that where electronic media (USB Storage Devices, CD/DVD etc.) containing sensitive company or customer data is to be sent via post or courier, the data contained thereon is encrypted (please contact the AMAZEING Support Helpdesk for further assistance)

c) wherever possible, ensure that sensitive information or customer data is 'double bagged' using two envelopes or packages with the details of the Metro Bank sender or recipient clearly visible on the inner bag (this is to help ensure that the contents are not lost if the outer bag is damaged or destroyed)

Note: for more details on how to handle different type of information when using postal system and couriers, see the Information Classification and Handling Minimum Standard and Asset Management Minimum Standard.

15 Physical security

Principle: all users must exercise precaution and take necessary steps to ensure their personal physical security and of their fellow colleagues and physical security of Metro Bank information assets, in Metro Bank premises, commuting or working remotely.

All users are issued with an identity badge on joining the Bank. This is for their use only and they must not share it with anyone else, including fellow colleagues. If they forget their pass, they must request a temporary one from facilities and reception.

You are the Bank's eyes and ears, and your alertness will help us keep our colleagues and FANS safe. If you see someone without a badge or someone you do not know, and you feel safe in doing so, approach them and confirm their identity and purpose for being on the Bank's premises. If you are concerned for your personal safety, contact Building Security or Facilities immediately.

Visitors should be escorted at all times. Unescorted visitors found in non-public areas should be escorted to reception or Facilities so that the colleague responsible for the visitor can collect them.

Users must:

a) always wear their identity badges when on Bank premises

b) immediately inform the local security team if they lose their badge

c) present their badge at entry gates to gain access to premises

d) report any suspicious person or activity (e.g., tailgating) to the security guard, Facilities, Physical Security Team or their line manager

e) visually check work areas for signs of tampering (e.g., cables removed, or unknown devices being attached to computer system) and report anything suspicious to the security guard, Facilities, Information Security Operations Team or their Line Manager.

To keep Metro Bank's premises secure and our customer's information safe, users must:

a) clear work areas of any sensitive information including documents, removable media, bank cards etc

b) lock away any sensitive items at night or if you will be away from your workstation for any length of time

c) log-off computers when not in use such as at the end of each working day

d) clear notice boards and flip charts of sensitive information after meetings

e) where possible use the ‘secure print’ function on printers and collect printer and photocopier output promptly and

f) check that windows and doors are locked and activate the burglar alarm if you are the last to leave at night.

All computers accessing the network will be configured to automatically invoke a password protected screensaver after ten minutes of inactivity. Users must not disable or extend the screen-saver time out period without approval from the CISO Team.

Note: physical security considerations must be considered when working remotely from Metro Bank premises including abroad as laid out in section 16. Remote Working.

Note: for further details see Physical and Environmental Security Minimum Standard and Colleague Security Minimum Standard.

16 Remote working

Principle: when working away from Metro Bank physical offices including working abroad, users must handle their devices securely and ensure that they are always protected.

In addition to the rest of the requirements within this Minimum Standard, where users are authorised to work remotely from Metro Bank premises, they must:

a) not leave Metro Bank devices and information unattended at any time. This includes any personal devices that contains or has access to Metro bank information e.g., through authorised BYOD (Bring Your Own Device)

b) whenever a Metro Bank device us not under your direct control (e.g., when stepping away for any reason) the device must be protected from theft (for example using a physical restraint such as a Kensington lock or by taking it with you)

c) if leaving devices such as laptops for short periods screens must be cleared and locked

d) completely switch off or hibernate their equipment when not using it for any substantial amount of time, e.g., overnight

e) always keep privacy screen in place to prevent shoulder surfing (These can be ordered through the Desktop Support team)

f) be aware of your surroundings to ensure that work-related conversations are not overheard by unauthorised individuals (e.g. when using mobile phones or other conferencing tools such as Microsoft Teams)

g) where the use of USB and other back up media has been permitted, ensure you keep them safe and separate from devices and equipment

h) not print any Metro Bank information to any printer that is not managed by Metro Bank unless you have been granted permission to use it through a request to Amazeing Support. (Typical examples of printers that must not be used include home printers, printers in hotels or internet cafés etc.)

i) not allow any non-Bank or other unauthorised individuals to use Metro Bank devices and equipment under any circumstances

j) not take Metro Bank devices and equipment outside UK (unless an exception has been agreed through the Working Abroad process) and any conditions agreed through that are fully complied with

k) never allow remote access to their machine by anyone other than AMAZEING Support and only then, after raising a ticked and being informed by the Amazeing Support team to expect a remote access session, must this allowed to happen. If you are unsure that the requester is authorised to act on behalf of Amazeing Support, please phone Amazeing Support on 020 3402 8888 to confirm

l) report any loss or theft of their equipment immediately via Amazeing Support, CRM (if possible) and to their line manager (who must arrange for it to be reported on CRM if you cannot do so)

The above applies to all computing equipment (Laptop, Tablet, Desktop, and Mobile) which is supplied by Metro Bank to colleagues and the BYOD devices which are controlled and configured by the Bank.

16.1 Working abroad

Please consult the Working Abroad page on Metropedia and information regarding the eligibility requirements, request process and other information relating to working abroad.

17 Reporting incidents

It is a responsibility of all users to report any observed or suspected information security and privacy incidents that may impact the confidentiality, integrity, or availability of Metro Bank information and / or its business interest.

The following events in relation to corporate devices and information are considered as reportable incidents, including but not limited to:

a) loss, theft, misuse, or suspected misuse

b) information and / or personal data accessed by an unauthorised third party

c) deliberate or accidental action (or inaction) by both authorised and unauthorised parties

d) sending information and / or personal data to an incorrect recipient (customer card, statement, correspondence)

e) alteration of information and / or personal data without permission

f) loss of availability of personal data

g) any unusual or unexpected activity that gives cause of concern.

Incidents must be reported via CRM or by calling the AMAZEING Support Service Desk on 0203 402 8888.

Note: there is no time to lose if a potential personal data breach has been identified. As part of the General Data Protection Regulation (GDPR), Metro Bank need to report potential or known data breaches to the Information Commissioner's Office (ICO) within 72 hours of initial discovery.

Note: as defined by the Information Commissioner Officer (ICO), personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes".

Note: if required, the incident should be reported by the colleague to the British Transport Police or Local Police and a crime reference number should be obtained.

Upon reporting an information security or privacy incident, Metro Bank reserves the right to perform a remote wipe to protect information stored on a corporate device. The remote wipe is enforced to prevent unauthorised access to both corporate data and the user own personal data.

Users must note that the remote wipe will remove all personal content in addition to all Metro Bank information.

Metro Bank is not liable for the loss or corruption of any personal data, software or other content stored on the corporate device. Users are encouraged to back-up their personal data on a regular basis.

18 Exceptions and dispensations

To accommodate new requirements or handle temporary operational issues, Metro Bank may grant exceptions and/or dispensations covering variance from or non-compliance with this minimum standard. Dispensations regarding any non-compliance to this minimum standard can only be authorised by the Chief Information Security Officer (CISO) or nominated deputy.

The above will not be approved where there may conflict with a legal or regulatory obligation (e.g., Prudential Regulatory Authority & Financial Conduct Authority, Payment Schemes (Faster Payments, BACS, Swift, Link, etc), Data Protection Act 2018, General Data Protection Regulation (GDPR) or Payment Card Industry – Data Security Standard (PCI-DSS).

For further guidance see Dispensation and Exception Minimum Standard.

19 Non-compliance

Metro Bank reserves the right to audit compliance with this Minimum Standard from time to time.

All violations of this standard will be reported to management. An internal investigation will be set up in accordance with People Team Policy to examine the detail of any security incident and will take any necessary actions including invoking disciplinary procedures where appropriate.

Failure to comply with this standard may constitute a breach of terms and conditions of employment or contract and can lead to legal or disciplinary action including dismissal or termination of contract.

Ignorance of standard requirements will not be accepted as mitigation for a security violation.

Colleagues are our best defence, and we rely on them to bump up any security concerns they have as soon as possible. Security of data, systems and services is a critical business objective for Metro Bank.

Users must Bump Up to their line manager inappropriate use of information, in addition to raising an Incident in CRM. If unsure, please Bump Up to infosecandcyber@metrobank.plc.uk or the Head of Information and Cyber Security.

20 Assurance

For this Minimum Standard to be embedded, it must be utilised in practice and be integrated within relevant business processes and procedures. To assess compliance and embedding, the following 1st, 2nd and 3rd line of defence processes must be followed to gain assurance that the Minimum Standards have been embedded and are being adhered to appropriately:

a) **Information Security Assurance:** Information Security Assurance within the CISO Team provides assurance that the Information Security Minimum Standards are implemented across the Bank through conducting design effectiveness assessments (DEA) and operational effectiveness testing (OET) of Information Security controls.

b) **Risk & Control Self-Assessment (RCSA):** at least annually or following a material change to the risk profile, the CISO team is responsible for identifying and assessing the risks inherent in their products, activities, processes, and systems, as well as the mitigating Key Controls in place, as defined and set out in the RCSA Standard.

c) **Control testing:** as outlined in the Controls & Testing Standard (which outlines the detailed requirements, definitions, and roles and responsibilities in this respect), in conjunction with the RCSA process, control owners are responsible for testing controls on a periodic basis and / or ensuring adherence to control objectives (broad requirements for controls).

d) **Compliance and Financial Crime Assurance:** Compliance and Financial Crime Assurance teams are each responsible for producing and delivering on the Combined Assurance Plan, in conjunction with Internal Audit as set out below. As part of the plan, the teams will assess the risk management activity and Key Controls across the Bank's 1st line of defence.

e) **Internal audit:** to provide effective 3rd Line assurance, internal audits will include testing the design and operating effectiveness of this Minimum Standard including the design and operating effectiveness applicable Key Controls.

For further details see Policy Governance Framework.

21 Training and awareness

The CISO Team maintains a communication strategy, working where appropriate with the Metro Bank University (MBU) and Metropedia Content teams, Enterprise, and Operational Risk Management. It details methods which are utilised to inform colleagues of this Minimum Standard, or its changes.

This Minimum Standard will be communicated to all colleagues and third parties in conjunction with required training in line with the InfoSec Training and Awareness Plan that is managed and maintained by the CISO Team.

This includes, but not limited to the following:

a) Information Security induction training including AUMS training and acceptance

b) MBU online training including annual re-acceptance of AUMS

c) Metro Bank M-Change security newsletters and bulletins

d) intranet-based security reminders

e) ad hoc training and communications in response to updates to this Minimum Standards and threats to Metro bank assets.

All training records are managed through MBU and are logged in the Learning Management System (LMS). Any additional training delivery mechanisms are recorded and managed by the CISO Team.

22 Acceptable use minimum standard acceptance

Colleagues accept this agreement during onboarding and complete it electronically as part of the annual MBU mandatory training.

Temporary staff, contractors, consultants, and other third parties are to complete, date, sign the section below and return it to the Hiring Manager who needs to complete it and submit before access will be provided.

Corresponding Metro Bank Contact/Hiring Manager is responsible for ensuring this agreement is completed properly and refreshed as necessary (at least annually and at contract extension or other material change for a third party carrying out services for Metro Bank.

I confirm that I have read Metro Banks Acceptable Use Minimum Standard and agree to adhere to its requirements:

Name:	
Signature:	
Date:	
Name of Parent Company:	

Metro Bank Contract / Hiring Manager:

I have ensured that the person named above has signed the Acceptable Use Minimum Standard.

Name:	

Signature:	
Date:	

Note: the acceptance form above will not be valid until both the third party and the corresponding Metro Bank Contract/Hiring Manager have signed it. The signature must be a wet signature, electronic or digital signature. A typed name is not acceptable and does not qualify as a signature.

23 Appendices

23.1 Microsoft multi-factor authentication (MFA)

To do MFA users are required to use either a hard token or a Microsoft Authenticator application. Some users such as cashiers and customer service representatives will be required to use hard tokens, whereas other store colleagues such as store managers and assistant store managers will be allowed to use mobile devices for MFA. Users in non-client facing roles would be expected to use mobile devices, but when it is not possible Metro Bank will issue a hard token.

Users must not share their hard tokens with anyone else, and handle them with caution to avoid damage, theft or being lost.

Microsoft Authenticator application can be installed on both Metro Bank and non-Metro Bank mobile devices and on up to five different devices.

All users must not share the use of application with anyone else and ensure that the mobile device is protected from unauthorised use and access.

Users that work on the store floors and other customer that are using mobile devices for MFA must be aware that there is are risks of security and privacy breaches, reputational damage and personal and physical security associated with the use of mobile devices in customer facing areas.

Hence, users must ensure the following to minimise these risks:

a) keep phones on silent while users are in areas where they interact with FANS (customer facing roles)

b) phones must not be looked at or in view at anytime, anywhere on the Store Floor except when the customer-facing users are at terminals and are required to authenticate. When users do use the phone to authenticate, they should make this clear to any customers they are serving to prevent any misunderstanding.

c) where possible, mobile phones should have voice recognition and recording apps switched off (SIRI, Google Assistant, etc).

d) users must be reminded of the correct behaviours and actions to be taken during various situations so not to endanger themselves, other colleagues, or FANS. This is even more important during emergency situations.

e) users are encouraged to enable the phone biometric functionality (e.g., fingerprints) as an additional factor when using the Microsoft Authenticator application. **Note:** This cannot be enforced by Metro Bank as we do not control the phone.

f) for their own security and to protect Metro Bank, users should ensure that they apply patches and updates to their phone operating system and applications as soon as possible after these are released. **Note:** This cannot be enforced by Metro Bank as we do not control the phone.

g) users must hand over phones for digital imagining by Cyber Investigation Team on request. (Phones will be returned after it has been fully imaged to help with investigations). **Note**: this will be challenging to manage, and we may not have the ability to enforce or manage practically, legally, or morally but it is important to recognise the potential risk and potential mitigations to allow a risk informed decision to be made.

23.2 Jargon Buster

For further details on applicable definitions see Jargon Buster on Metropedia.