OmnicomGroup

Bring Your Own Device Policy

Bring Your Own Device Policy ("the Policy")

Contents

Part 1 - Introduction

What is the purpose of this Policy?

Omnicom and its Agencies strive to attain a high standard of information security in order to protect information and personal data that we hold about our business, clients and employees ("Omnicom and Agency data").

Information about our security standards and general approach to data protection can be found on Omnicom's IT Central site at https://oneomnicom.sharepoint.com/sites/OMC-ITCentral/SitePages/Policies.aspx

When you access the systems of Omnicom or an Omnicom Agency using a mobile device, we are exposed to a number of risks, including the risk of loss or theft of the mobile device (which could result in unauthorized access to systems) or the threat of malware (such as viruses, worms, spyware, Trojans or other threats). We are also exposed to the potential loss or unauthorized alteration of Omnicom and Agency data which could in turn expose us to the risk of non-compliance with our legal obligations in terms of confidentiality, data protection and privacy. Such risks could result in damage to our systems, business, clients and reputation.

We recognise that many of our employees have personal mobile devices (such as tablets, smartphones and handheld computers), which they wish to use for business purposes, and that there can be benefits for both us and employees, including increased flexibility in our working practices, in permitting such use.

As such, you may be able to use your personal mobile device for work purposes subject to (a) obtaining our authorization; and (b) complying at all times with this Policy and any related policies and processes including the:

- Acceptable Use Policy.
- User Information Security Manual.
- Mobile Device Management (“MDM”) Terms of Use and Privacy Statement.
- Data Protection (Staff Responsibilities) Policy.

These policies can be found here: https://oneomnicom.sharepoint.com/sites/OMC-ITCentral/SitePages/Policies.aspx

Scope

This Policy applies to anyone who uses a personal mobile device for work purposes, to access/connect to our systems or to store or access any Omnicom and Agency data. This includes all employees, officers, volunteers, interns, casual workers or agency workers plus any consultants, contractors or freelancers (whether retained directly or using a personal services company). When we use the terms ‘employee’ or ‘employment’ or ‘engagement’, we mean all these categories of workers.

For the purposes of this Policy, **"mobile devices"** include but are not limited to mobile phones, tablets, laptops, mobile hotspot devices, Internet-based technology such as Alexa, and wearable technology. Unless otherwise specified, when we talk about mobile devices in this Policy we are talking about personal mobile devices (not corporate-owned devices – these are covered by our Acceptable Use Policy and MDM Terms of Use).

When we talk about our **"systems"** we mean the IT and communications systems, software, servers, computer hardware of Omnicom and its Agencies.

When we talk about **"corporate productivity tools"** we mean the tools and applications you use as part of your work including: Outlook, Teams etc.

This Policy is intended to comply with applicable laws and regulations in each country within which we operate. If the Policy permits or prevents an action that is not permitted by local laws and regulations, the requirements of such local laws and regulations will be followed.

Compliance/Enforcement

Breach or suspected breach of this Policy may lead to us revoking your access to our systems, whether through a mobile device or otherwise. It may also result in disciplinary action up to and including the termination of your engagement with us. Where appropriate, performance improvement processes may also be undertaken. Such action may be taken whether the breach is committed during or outside office hours and whether or not use of the mobile device takes place at your normal place of work. You will be required to co-operate with any investigation into a suspected breach, which may involve providing us with access to the mobile device and any relevant passwords and login details.

Part 2 – Core Obligations and Information

Use of your mobile device for work purposes is subject to the following requirements:

1. Authorization Requirements

- All mobile devices falling within this Policy must be registered with and approved for use by Omnicom Security Services via the Paige support tile in the Governance, Risk and Compliance section of the intranet. **You must do this before you can use your mobile device under this Policy.** Enrolment of the mobile device in Omnicom's Mobile Device Management solution (MDM) and compliance with our MDM Terms of Use is required as a condition of any authorization.

2. Your Obligations

- You may only access our systems, including any corporate email/productivity tools, via the MDM. The MDM settings on your Device should never be altered without written consent from Omnicom Security Services. Any settings designed for the protection of our staff, your Agency and your clients. If the MDM settings are causing issues on your mobile device you must speak to Omnicom Security Services and should not simply try to disable or change them.

- When accessing any of our systems or corporate productivity tools, or otherwise using your mobile device for any Omnicom or Agency work, you must comply with Omnicom and Agency's Data Protection (Staff Responsibilities) Policy, Acceptable Use Policy and the Omnicom Information Security Policy and any other policies covering use of our systems, IT security or data protection. This includes your use of email, apps, the internet and social media.

- You must comply with our mobile device configuration requirements and install any security software or security-related applications requested by us. Our mobile device configuration requirements include ensuring mobile devices are encrypted and utilising a secure access method: either a password, pin, or biometric access controls. Your password must be a secure password that complies with Omnicom's Password Policy, which can be found in the User Information Security Manual. We require that mobile devices automatically lock (requiring unlock via a secure access method as above) if idle for five (5) minutes or above. You must not alter these or other security settings on the mobile device or MDM, including trying "jailbreak" the device.

- You must at all times use your best efforts to physically secure the mobile device against loss, theft or use by persons who we have not authorized to use the device. You must secure the mobile device whether or not it is in use and whether or not it is being carried by you.

- You must prohibit and ensure there is no access to our systems or corporate productivity tools on the mobile device by anyone not authorized to use it by us, including family and friends.

- All Omnicom and Agency data should be strictly kept within corporate productivity tools which are accessed through the MDM. This information must **not** be kept outside of these tools or on other areas of your mobile device. Personal email accounts/services should **never** be used to hold/process Omnicom and Agency data.

- You must only access and download data which is necessary for your role, as per the Omnicom Acceptable Use Policy. You must not copy, save, forward or otherwise process confidential information or intellectual property, including trade secrets, on a mobile device unless such action is strictly necessary for business purposes.

- You must not back up or otherwise store Omnicom and Agency data to a personal or non-authorized cloud-based storage system or service (such as DropBox, Google Drive, personal OneDrive, iCloud) without our written consent (as described in the Omnicom Acceptable Use Policy). Any such backups or other stored copies inadvertently created must be securely deleted as soon as you become aware of them.

- If you leave employment from Omnicom or an Agency, you must follow any instructions given to allow us to remove any Omnicom and Agency data and corporate productivity tools from your mobile device. If requested, you must promptly give the mobile device to the IT Department and provide any password, pin number or similar to allow any Omnicom and Agency data to be removed from the mobile device.

- By using your mobile device for work purposes, to access our systems, or to store or process Omnicom and Agency data, you acknowledge that any information accessed, stored or recorded for the purposes of (or in relation to) any work you do for us or our clients (including any Omnicom and Agency data) is our property, regardless of who owns the mobile device.

3. Costs of use

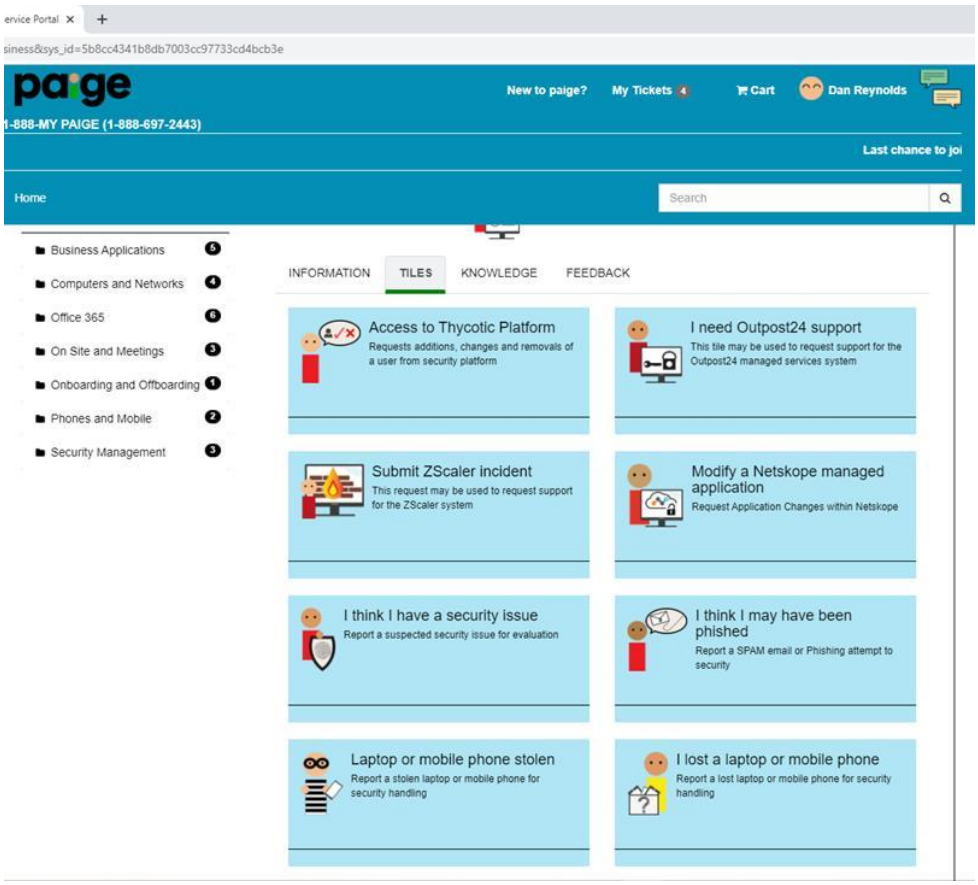
- Except as otherwise specified to you by Omnicom or your Agency, you are responsible for all expenses incurred using your mobile device. Expenses include, but are not limited to: monthly access fees, roaming charges, usage fees of any kind, application purchases, in-app purchases, taxes, etc.

- Omnicom does not provide mobile device insurance and you are responsible for insuring your device.

- If you are travelling for work to places which may lead to additional costs relating to your mobile device, you should speak to your Agency in advance and agree the parameters for use.

4. Lost Mobile devices

- If your mobile device is lost or stolen, **<u>you must act immediately</u>**. You should **notify us using the 'Laptop/Mobile phone lost or stolen' tile below** OR **email** SOC@omnicomsecurityservices.com



- Appropriate steps will then be taken to ensure that Omnicom and Agency data on or accessible from the mobile device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all Omnicom and Agency data on the mobile device (including all information contained in a work e-mail account, even if such e-mails are personal in nature). Although we do not intend to wipe data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from Omnicom or Agency data in all circumstances and you must be aware of and accept the risk that personal content may be lost if you are using your mobile device for work purposes. However, this must not be a reason for not reporting a mobile device lost.
- For more information about Security Incident and Data Breach reporting please see our Acceptable Use Policy.

Monitoring and Access to Information

Once you start using your mobile device on our systems, your system usage and the data processed in connection with that use may be recorded (again, even if the use relates to personal content) by virtue of how our systems function. For this reason, and in the course of exercising our rights under this Policy, we may (subject to local laws) access and otherwise process personal content on your

mobile device even if marked “personal”. You are therefore advised not to use your mobile device on our systems for any matter intended to be kept private and/or confidential.

In particular, we may (without further notice or your express permission always subject to local laws) inspect your mobile device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the data. We do this only where necessary for legitimate business purposes including (without limitation):

- to maintain the security of our systems;
- to protect Omnicom and Agency data;
- to comply with any relevant regulatory or legal obligations (including in relation to confidentiality, data protection or privacy); and
- to ensure compliance with our rules, standards of conduct and policies in force from time to time (including this Policy).

As above (and again subject to local laws) the data that we use, access, remove or copy may include personal content unless it can be easily isolated from non-personal content.

For more information about how we process your personal data when using our systems – including more information about why we monitor our systems and how we do this - please see your relevant Workplace Privacy Notice and the Omnicom Acceptable Use Policy.

Part 3 – Governance Information and Policy Management

Created	6/1/2018
Last Reviewed	11/19/2020
Version	1.0
Scope	This document contains Omnicom's policy on using personally owned computing mobile devices in the process of doing day to day business.
Location(s)	Applicable Worldwide (subject to laws in each jurisdiction)
Document Classification	Internal
Reviewed and Approved By	Omnicom Information Risk Management Committee

Responsibility

The Omnicom Information Risk Management Committee is responsible for the administration of this Policy. If you have any questions regarding this Policy or if you have questions about items not addressed in this Policy, please contact your Network CISO.

Policy Distribution

This Policy will be provided to new joiners, either by their local HR or IT Support. The Policy will also be sent to all employees annually. This is the responsibility of Omnicom Security Services. The Policy can always be found on the intranet.

Changes to this Policy

The Policy is a living document. As such, it will be periodically reviewed and updated to maintain applicability and alignment with Omnicom business practices and applicable laws, regulations and guidance.

Further revisions of the document will be presented to the Information Risk Management Committee for review and approval. Revisions of the document shall supersede all previous versions.

The signatures of two members of the Information Risk Management Committee are needed to authorize any material revision. Authorizations are set out at Part 4 below.

Revision History

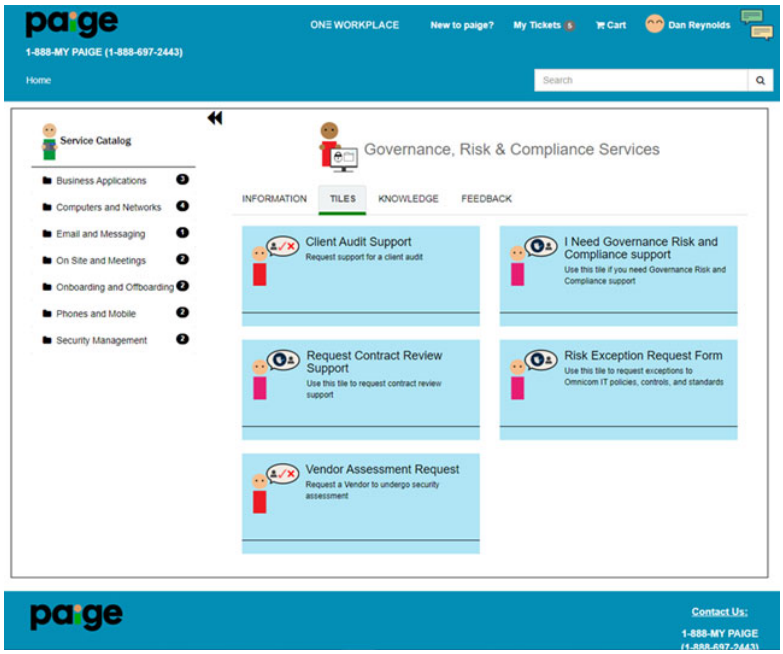
Version	Date Signed	Date Effective	Description
1.0	11/19/2020	11/19/2020	Initial Policy

Exceptions to this Policy

Exceptions can only be made to this Policy with specific authorization from Omnicom Security Services.

Typically, exceptions to this Policy can only be made in very limited circumstances and will only be granted following a review by Omnicom Security Services.

Exception requests should be made to Omnicom Security Services by completing the Omnicom Risk Exception Request form on the Paige Service Portal as set out below. The department making the request must have CFO approval as well as approval from Omnicom Security Services.



Part 4 - Authorizations

The Information Risk Management Committee of Omnicom has reviewed this Policy and agrees that it aligns with our fundamental business goals and professional ethics. In good faith and with all due authority, we, the undersigned, sign this Policy into effect, the effective date noted in the revision table. The Policy is authorized and to be enforced as part of our normal daily operations.

Paul B. Scott
Paul B. Scott (Nov 30, 2020 21:18 GMT)

Nov 30, 2020

Paul Scott

Global Chief Information Security Officer

Deputy Chair, Information Risk Management Committee

Date:

Craig Cuyar (Nov 30, 2020 20:28 EST)

Nov 30, 2020

Craig Cuyar

SVP and Global Chief Information Officer

Chair, Information Risk Management Committee

Date: