OmnicomGroup

ACCEPTABLE USE POLICY

ACCEPTABLE USE 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"). The Omnicom Acceptable Use Policy (the "AUP" or the "Policy") sets out our commitment and strategy in managing information security risks and ensuring proper use of our IT systems.

Improper use or unauthorized access to our systems can expose us to a number of risks, including the threat of malware (such as viruses, worms, spyware, Trojans or other threats), the potential loss or unauthorized alteration of Omnicom and Agency data and 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. This Policy is therefore essential in maintaining Omnicom's competitive edge, profitability, legal compliance, and commercial image.

What is information security?

In this Policy **"information security"** refers to protection of the confidentiality, integrity, and availability of information across our systems from the threats outlined above – this includes preventing data loss, theft and corruption as well as countering its unauthorized use, copying, or modification, whether by deliberate means or by accident.

Information security involves applying an appropriate set of administrative controls (including policies, standards, guidelines, and procedures) in combination with physical and technical controls. These controls must be implemented, monitored and reviewed to manage information security risks and protect our business, our clients and our employees. This Policy is part of the way we manage those controls.

For the purposes of this Policy:

When we talk about our **"systems"** we mean our IT and communications systems, including our networks, software, servers and devices (as defined below).

When we talk about **"devices"** or **"assets"** in this particular Policy, we are talking about any technology that connects to or otherwise interacts with our systems or which holds, accesses or otherwise processes Omnicom and Agency data. This includes "**mobile devices"** (which include but are not limited to mobile phones, tablets, laptops, mobile hotspot devices, Internet-based technology such as Alexa, and wearable technology), the computer systems and hardware in our offices (such as desktop PCs) and peripheral equipment and storage devices.

Where do you come in?

Managing information security risks requires the commitment, participation, and accountability of Omnicom's employees and business partners. It is therefore vital that you follow this Policy and all other policies governing our approach to information security and data protection, including the:

- User Information Security Manual

- Bring your own device ("BYOD") Policy
- 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 performing services for or on behalf of Omnicom Group, its Networks, Agencies, Affiliates, Associations, and Subsidiaries (or for any Clients of any of these) so far as those services involve using or accessing our network or systems, or otherwise accessing or processing 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.

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. 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 the breach 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 any relevant device and any relevant passwords and login details.

Part 2 – Core Obligations and Information

You are responsible for taking all reasonable steps to prevent the unauthorized disclosure or compromise of Omnicom assets, systems, and data. It is your responsibility to ensure that you are familiar with the obligations in this Policy. You must also review the above policies plus any security policies and user manuals relevant to your role (at least annually).

1. General Security Principles

The following are some of the core obligations you should be aware of. These are expanded on in the sections below.

- You must act with professionalism, honesty, and integrity when using Omnicom technology resources, data, devices and systems.

- You must ensure that devices and systems are kept secure – including using appropriate passwords and (where appropriate) encryption processes. Devices should be locked when idle, and you should not permit unauthorized users. Omnicom provides a solution for secure encrypted password recovery and you must enroll in this system any device that will hold Omnicom or Agency data. Our Password Policy and encryption requirements can be found in the User Information Security Manual.

- You should be aware that when using devices away from the workplace, documents may be read by third parties, for example, passengers on public transport, and take all necessary steps to prevent this. This may include shielding your screen or waiting until a more appropriate time to access the information.

- You must be aware of the wireless networks you connect to - avoid connecting to suspicious or unknown wireless networks while out of the office. Where possible, use a company-issued mobile "hot spot". Always use the Omnicom VPN for extra security.

- You must not install software or applications (or connect to any devices) not authorized by us, especially from unknown or untrusted sources.

- You must ensure there is no access to our systems or corporate productivity tools on any device by anyone not authorized to use it by us.

- You must not open suspicious or unsolicited emails, attachments, or website links that do not appear legitimate. If you are unsure about any questionable content, contact Omnicom Security Services.

- You must tell us immediately if you think there has been a security incident or a data breach, following the guidance set out below.

- Before using a mobile device for work purposes, to access our systems, or to otherwise access or process Omnicom and Agency data you must read, agree to and comply with the terms of the Mobile Device Management User Acceptance Form and Privacy Notice and (if it is a personal device) the BYOD Policy.

2. Protecting Physical Assets

You are responsible for safeguarding devices under your control to avoid their loss or theft. This includes taking the following steps:

- Securing devices at all times when not in use. This will mean as applicable (based on the type of device):
    - securing the device with a cable lock if available;
    - locking devices in your cabinet drawer; and
    - taking devices home.

- Avoid leaving devices unattended in public places or your car. If there is no other option but to leave a device in a car, keep it locked in the trunk and ensure it is out of sight.

- Report any lost or stolen devices as per the instructions in the 'Reporting Security Incidents and Data Breaches' section below.

3. Passwords

All Omnicom and Agency systems require a unique login and password to gain access. You must use a password that meets the requirements of our Password Policy. This is set out in the User Information Security Manual.

4. Removable Media

All removable media (e.g., DVDs, USB thumb drives) used for work purposes or to store or transfer Omnicom or Agency data must be encrypted and protected by a password. Please contact your Agency IT department or the Paige Service desk for assistance.

5. Information Storage and Cloud Services

You must only use approved storage solutions. These are as follows:

- Teams
- OneDrive
- A Company owned network server shared drive

You must **not** use public or personal cloud storage services (e.g., DropBox, Google Drive, personal OneDrive, iCloud) to store for work purposes or to store or transfer Omnicom or Agency data. You must request a formal exception if you believe you need to use one of these services for business purposes. Instructions on how to do this can be found in Part 3 below.

The temporary storage of Omnicom or Agency data on your mobile devices is permissible for conducting Omnicom business while traveling. However, this should be limited to what is necessary for business purposes and bulk exporting or downloading files from Omnicom or Agency systems is not permitted. If you need to obtain copies of a file, contact Omnicom Security Services for guidance.

6. Digital Information Transfer

You should take special care to ensure that any Omnicom and Agency data is appropriately protected when sent by electronic means and that said data is sent only to those authorized to receive it.

You should ensure that you use only our approved data transfer methods. Further information is set out in the User Information Security Manual.

In addition, specific types of confidential information (for example, sensitive personal data, or client intellectual property) must not be digitally transmitted unless encrypted by Omnicom-approved encryption software. Further information is set out in the User Information Security Manual

The use of, installing or running "peer-to-peer" file-sharing software (for example Bit Torrent, U Torrent or Limewire) is prohibited.

The importing or exporting of mailboxes (PST files) into or out of Omnicom email system is prohibited without permission from Omnicom Security Services. This may be granted subject to supervision from Omnicom Security Services.

7. Data Classification Policy

We have implemented a Data Classification Policy which contains specific rules on the storage and transfer of different types of data. This is set out in the User Information Security Manual. You must review and comply with the Data Classification Policy.

8. Email and Other Electronic Communications

You should adopt a professional tone and observe appropriate etiquette at all times when using Omnicom systems to communicate with others. In addition, you should comply with the following obligations:

- Do not use your personal accounts (for example your personal Hotmail, or Gmail account) to send or receive communications (including email) for the purposes of our business and do not forward any Omnicom and Agency data to your personal accounts. Only use the accounts we have provided for you.

- Do not use instant messaging ("IM") technology other than those we have approved. The current approved IM platforms are Skype, Teams, and Jabber.

- Texting messaging (SMS) is not a secure means of communication, and you should not send Omnicom and Agency data via SMS.

- You should not send or forward communications (including email) using our systems which you would not want a third party to read, or on respect of which you have an expectation or assumption of privacy. For reasons set out below these communications cannot be presumed to be private.

- You should not send communications (including email) from another employee's account, device or under an assumed name unless specifically authorized to do so.

- Matters of a sensitive nature should not be transmitted by email unless absolutely unavoidable and, if so, should be clearly marked as 'confidential'. Client emails should always be marked as 'confidential'.

- You should not agree to any term or enter into contractual commitments or make legal representations by email unless appropriate approval has been obtained. If you are unsure

about this you should speak with your manager or Network/Practice Area General Counsel in the first instance.

- If you receive a wrongly delivered email you should let the sender know as soon as possible. If it contains confidential information or inappropriate material (as described above) it should not be used or disclosed in any way. You must also inform Omnicom Security Services about the communication.

- You should try your utmost to ensure that communications (especially email) are sent to the correct recipient. If you send an email to the wrong recipient, you should follow the instructions in the 'Reporting Security Incidents and Data Breaches' section below.

Remember that written communications (including email) can be used in legal proceedings or be released as part of a "subject access request" under privacy law (both staff members and customers may make such requests). Even "deleted" communications may remain on our systems and be capable of being retrieved. A good rule to follow is to assume that email messages may be read by others, and do not include anything which would offend or embarrass any reader, yourself, or us if it found its way into the public domain.

9. Disposal of Physical Assets

You should dispose of any paper documents in designated shred bins or shredders located throughout your assigned facility. Before disposal, ensure that information does not need to be retained for business purposes. If you are unsure, contact your manager or your local document retention administrator for guidance. Where you are working from home, ensure that you exercise due diligence and care when printing and disposing of paper documents.

Electronic media (e.g., hard drives, DVDs, USB thumb drives) must be securely erased or physically destroyed; please contact your local IT Service Desk for assistance.

10. Traveling Outside of the Office

When traveling, do not check laptops or mobile devices in hold luggage of an airplane (unless the relevant authorities mandate this). Instead, carry laptops and mobile devices with you. When traveling, never use shared computers (for example, those in hotel business centers and cyber cafes) to log into our systems. These public-use computers can be infected with spyware, viruses, or malware that work to capture your keystrokes and passwords when entered. If you will need to access our systems when traveling, and do not have an appropriate corporate device and are not set up under our BYOD Policy, please speak to your local IT Service Desk for assistance.

11. Bypassing Security Controls

The security controls we put in place for our assets, devices and systems are important parts of our overall information security strategy. As such you must not:

- attempt to tamper with, modify, disable, or bypass security controls to gain unauthorized or elevated access to data, information, assets, or facilities;
- install software or hardware that bypasses, disables, or interferes with security controls at our offices, such as wireless access points; or
- use an account owned by another user without their knowledge or permission.

12. Prohibited Activity

Inappropriate use of Omnicom or Agency systems in breach of this Policy or our other policies can be dealt with as a disciplinary matter. Misuse of the internet can also in some cases be a criminal offence in addition to being a disciplinary matter.

Creating, accessing, transmitting, sharing and/or downloading (as relevant) any of the following material can amount to gross misconduct (this list is not exhaustive):

- pornographic material (that is, any media of a sexually explicit or arousing nature);
- offensive, discriminatory, obscene, derogatory or criminal material or material which is liable to cause embarrassment to us or our partners;
- a false or defamatory statement about any person or organisation;
- unauthorized software, including but not limited to malicious programs (e.g., viruses, worms, Trojan horses, email bombs, etc.);
- any material which would breach any of our other policies or otherwise be contrary to our interests.
- any other statement which is likely to create any criminal or civil liability (for you or for us) including by breaching copyright by downloading "pirated" software;

In addition, the transmitting and/or sharing of confidential information or personal data about Omnicom, our Agencies or any of our staff or clients except as authorized in the proper performance of your duties will usually amount to gross misconduct. Such confidential information includes, but is not limited to, the following examples: compensation, service development plans, buying rates, financial information, marketing strategies, pending projects and proposals, research and development strategies, plans for demonstration, advertising, and operations. For more information about your responsibilities in terms of personal data, please see our Data Protection (Staff Responsibilities) Policy.

13. Personal Use

We permit limited use of our systems to send personal email and browse the internet subject to certain conditions set out below and any particular restrictions your Agency puts in place. We may withdraw permission for this at any time or restrict access at our discretion. As set out further below, you should be aware that personal use of our systems may be monitored and where appropriate disciplinary action may be taken. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive or inappropriate.

Your personal use must meet the following conditions:

- must be appropriate and not interfere with business or office commitments;

- must comply with this Policy and Omnicom's other policies; and

- any personal message, email, folder, document and/or other data, whatsoever its format, created, received, sent, and/or accessed through the use of Omnicom systems should be identified "Personal". However, as we monitor our systems it is possible that even documents marked "Personal" may be accessed in some circumstances. Please be aware of this when choosing to put personal content on or access Personal content using Omnicom systems (see section 'Monitoring' below).

You are responsible for the management of any data that you create and store on our systems as a result of your personal use and neither Omnicom nor your Agency shall be held liable in cases of loss or destruction of such data.

14. Personally Owned Devices (Bring Your Own Device)

Omnicom supports a "Bring Your Own Device (BYOD)" environment. The conditions for using a personal device at work are detailed in the BYOD Policy which is complimentary to this Policy. You should obtain authorization under the BYOD Policy before using your own device for work purposes, accessing /connecting to our systems, or otherwise storing or accessing any Omnicom and Agency data of any personal device. You must comply with your ongoing obligations under the BYOD Policy for as long as you use your personal device for these purposes.

15. Monitoring

We may monitor, access, examine, capture or otherwise intercept ('**monitor**') (by human or automated means) communications or data transmitted through our systems. This may take place for a number of reasons, including to:

- maintain the security of our systems;
- identify and deter system security threats;
- protect Omnicom and Agency data;
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this Policy).
- locate deleted messages or messages lost due to system failure;
- manage and redistribute the work on an absent employee as needed;
- assist in the investigation of alleged wrongdoing;
- ensure that information is protected and has not been compromised;
- comply with any relevant regulatory or legal obligations (including in relation to confidentiality, data protection or privacy);
- improve and enhance the safety of staff and visitors;
- protect our premises and property (and the property of staff and visitors) from criminal activities;
- facilitate the identification, apprehension and prosecution of offenders; and
- for the purposes of establishing, exercising or defending legal claims.

Monitoring activities that we may undertake for these purposes may include:

- logging and storing internet usage including details about usernames, time spent on websites and the names of visited websites;
- blocking access to different categories of prohibited websites, such as gambling sites, pornographic websites, sites relating to criminal activity, or social networking or similar types of websites;
- logging all emails sent and received using our systems, including information about the sender, receiver, subject, time and size of the message and name of attached files;

- inspecting the content of certain emails to identify a threat to information security (e.g. virus attacks), or if it is necessary in order to investigate a suspicion of crime, breach of contract or protection of confidential information. The content of emails may also be checked when you are absent from work to enable work continuity.
- monitoring for malicious activity on our premises, systems and cloud services, for example by using proactive detection technologies which automatically flag suspected data leakage, data exfiltration or the use of malware.

When using our systems, emails or text messages that are private or marked "private" or "personal" (e.g. in the subject line or because they are stored in a folder marked "private" or "personal") may still be monitored, although we would try to avoid this where possible. Please note that the fact that a document, voicemail, data or communication has been "deleted" does not mean that the item cannot be retrieved and reviewed.

Targeted monitoring (that is monitoring directed at a particular individual) would normally only take place where there are reasonable grounds to suspect that criminal activity or serious misconduct is taking place and where, after suitable consideration, we reasonably believe there is no less intrusive way to address the issue. Only limited numbers of people will be involved in any covert or targeted monitoring and access will be granted for a short a time as possible.

For details of how this section applies when using your personal device for work purposes, please see the BYOD Policy.

16. Reporting Security Incidents and Data Breaches

It is important that you make us aware of and deal with any security incidents and data breaches that occur as part of your work.

A **"data breach"** occurs where there is destruction, loss, alteration or unauthorized disclosure of or access to *personal data* (defined as data relating to a living individual) which is being held, stored, transmitted or processed in any way. For example, there may be a data breach if you lose a laptop or a USB stick or if you send an email to the wrong person by mistake, depending on whether the USB stick or email in question contains personal data.

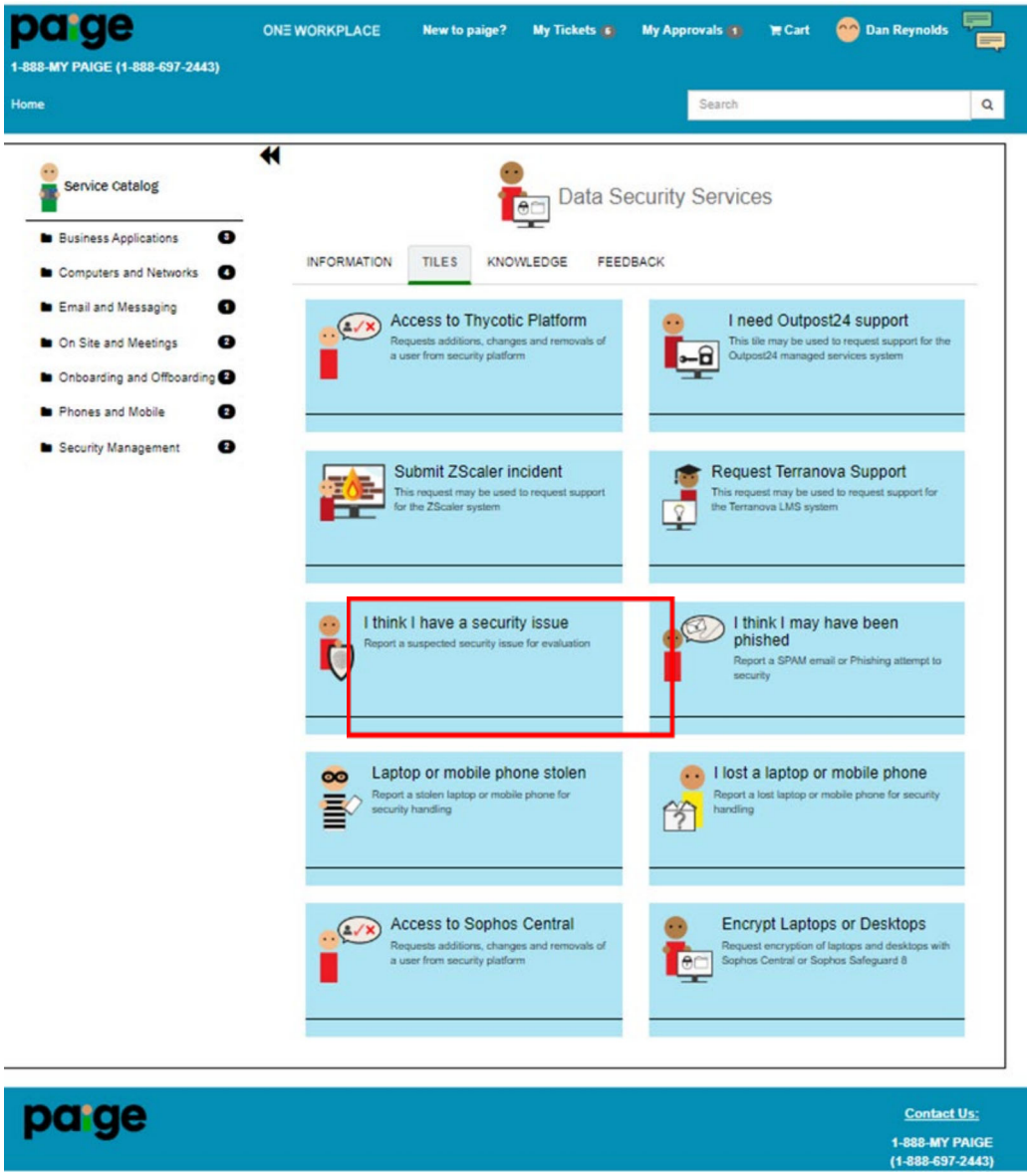
A **"security incident"** refers to any event resulting in a breach of security or unauthorized access to or acquisition, release, use, or disclosure of Omnicom and Agency data (even if this does not include personal data). Data breaches will typically also be security incidents, but security incidents can occur which do not involve personal data. Examples of the latter could include:

- strange or abnormal activity such as pop-ups on your workstation or laptop; or
- any suspected or known unauthorized disclosure or use of confidential *corporate* information.

Reporting Security Breaches

If you suspect there has been a security incident this **must** be reported **immediately** to Omnicom Security Services via the following methods:

- Email to SOC@omnicomsecurityservices.com; or
- completion of the appropriate service tile on the Paige service portal as set out below.



Reporting Data Breaches

If you believe that the security incident may also be a data breach, you **must** notify Omnicom Security Services **immediately.** You can do this by going to the Paige portal to report a security incident as above, or by emailing SOC@omnicomsecurityservices.com.

You may also notify your Chief Information Security Officer/Data Protection Officer.

No-one feels good if they leave a laptop on a train or if it is snatched from them in the street. Losing the data or exposing it to risk is much more important to us than losing the equipment. Do not delay – report it! As an organisation we may need to notify personal data breaches to the relevant regulator within a tight timeline: 72 hours. As such, failure to notify either a security breach or a data breach, or to provide follow up information as requested, will be treated seriously and disciplinary action may be taken.

Part 3 – Governance Information and Policy Management

Created	6/1/2018
Last Reviewed	19/11/2020
Version	3.0
Scope	The document covers the Company's policies on the acceptable use of technology
Location(s)	Applicable Worldwide (subject to laws in each jurisdiction)
Document Classification	Internal
Review 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

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 at least 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

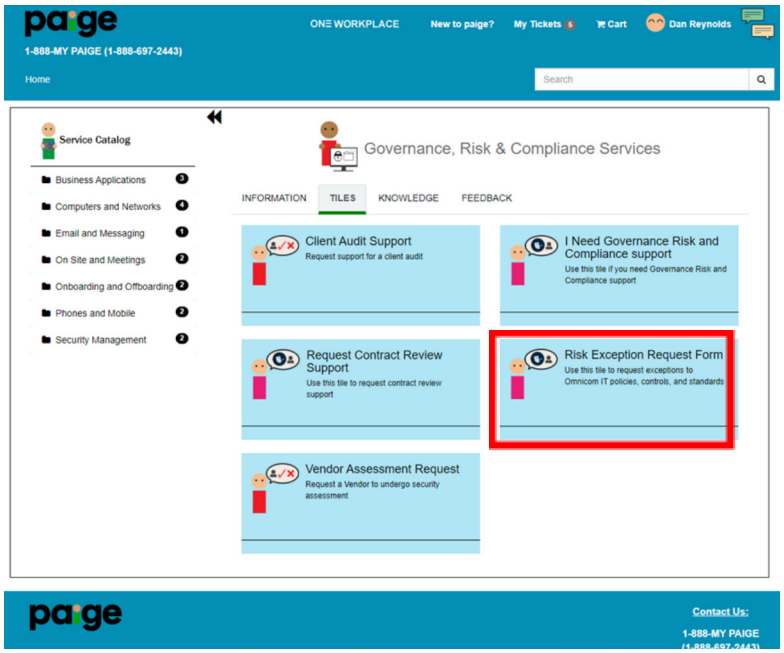
Version	Date Signed	Effective Date	Description
1.0	6/1/2018	6/1/2018	Initial Policy
2.0	8/15/2019	8/30/2019	Annual review – formatting changes, added supporting direction sections, modified terms – track changes on
3.0	11/19/2020	11/19/2020	Review and update

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, from the Effective Date noted in the Revision Table above. The Policy is formally authorized and shall be enforced as part of our normal daily operations.

Paul B. Scott
Paul B. Scott (Nov 30, 2020 20:56 GMT)

Nov 30, 2020

Paul Scott

Global Chief Information Security Officer

Deputy Chair, Information Risk Management Committee

Date:

Craig Cuyar (Nov 30, 2020 20:37 EST)

Nov 30, 2020

Craig Cuyar

SVP and Global Chief Information Officer

Chair, Information Risk Management Committee

Date: