Document ref	ISMS202107
Version	2
Dated	15/09/2020
Document author	Sarah Stobbs
Document owner	Mike Stobbs, Mosaic FSI
Approved by	Mike Stobbs
Confidentiality level	Internal

Version	Date	Revision Author	Summary of Changes
2	22/12/2020	Russell Fielding	Change format, update policies added social media awareness article.

IT and Social Media

We understand that using information technology (IT) can help you do your job and balance your work and life. But it should not interfere with your work duties or harm the business.
The policy sets out what is an acceptable use of IT and applies to:

- All employees, contractors and subcontractors who use our technology and systems.
- Wherever and whenever our IT and systems are used — on-site or away from work.
- During work time and out of work time.
- Work IT, personal IT used at work, or for work and any other IT used for work purposes.

As an employee and representative of Mosaic FSI, you are expected to demonstrate best practices and appropriate etiquette on social media, including but not limited to, the following:

What Mosaic's policy is

You must use IT and systems responsibly and reasonably. Your use must not interfere with your work duties, harm our business or other people, or be illegal.
This means you cannot:

- Harm our business or its reputation.
- Infringe rights or the law.
- Cause legal problems for Mosaic FSI, e.g., defaming someone or making false claims.
- Harass, bully, or offend anyone.
- Disclose any confidential information about Mosaic FSI, customers, clients or other private or confidential information except as is lawfully required by your job.
- Risk the security, safety, or ability of our systems, e.g., by downloading, streaming, or storing music, video, or images or by opening suspicious or unexpected attachments except as is lawfully required by your job.

You are also responsible for:

- Any damage or loss resulting from the misuse of technology. Keeping all work information, e.g., contact information, files, and emails, secure.
- Keeping any work devices safe and secure when they are outside the workplace.

Hardware and Software

You can use our hardware and software — including PCs, tablets, cell phones data sticks, compact discs, digital files and information, operating systems, programs, apps, and social media. You can use our internet access, including Wi-Fi, if you:
• Use software and hardware we have approved
• Keep passwords secret and hard to guess
• Keep our Wi-Fi user names, access codes and passwords confidential. You cannot view or download material, or visit websites that could be thought offensive, inappropriate or illegal.

You can use our computers and internet connection for personal use if it is at a reasonable level and doesn't make you less productive.

Email

If you use our work email account(s), you must meet the house rules set out at the start of this policy. You must:

- Only use email accounts you have permission to use.
- Meet New Zealand's anti-spam rules when sending emails to multiple addresses, e.g., marketing messages to customer lists.
- Get permission before you send unsolicited electronic messages to people, e.g., marketing, or promotional material.
- Use of Mosaic FSI resources for non-authorised advertising, external business, spam, political campaigns, and other uses unrelated to Mosaic FSI business is strictly forbidden.
- All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of Mosaic FSI.
- Employees should use only company-approved devices to access company email accounts.
- Employees must not use public devices such as those provided by hotel business services to access company email accounts.
- In no way may the email resources be used to reveal confidential or sensitive information from Mosaic FSI outside the authorised recipients for this information.
- Using the email resources of Mosaic FSI for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is not allowed at any time.
- Use of Mosaic FSI email resources are maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the user must deactivate the associated account according to established procedures for the accounts' lifecycle.
- Scanning technologies for virus and malware must be in place in PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
- Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.

Social Media

Use of our work social media account(s) must meet the house rules set out at the start of this policy. You can:
- Access and use social media using our IT for personal use at work during agreed break times.
- Access and use social media using our IT for personal use outside employment as long as it is reasonable.

All Employees must read the illustration at the bottom of this document regarding the security risk of social media.

Mobile Devices

We may lend you a mobile phone and/or laptop. Your use of our devices must meet the rules set out at the start of this policy.

- You cannot view or download material or visit websites that could be thought offensive, inappropriate or illegal.
- You must keep the phone/mobile device safe and secure. It must have a password that is secret and hard to guess.
- You may have to pay to replace a device you lost or damaged either on purpose or because you were careless.
- Never let other people use your device unless we allow you to.
- You must return the phone and/or laptop to us if we ask you to or when you stop working for us. We will keep ownership of the device — and its number if it's a phone — unless we agree otherwise.

Photos and Videos

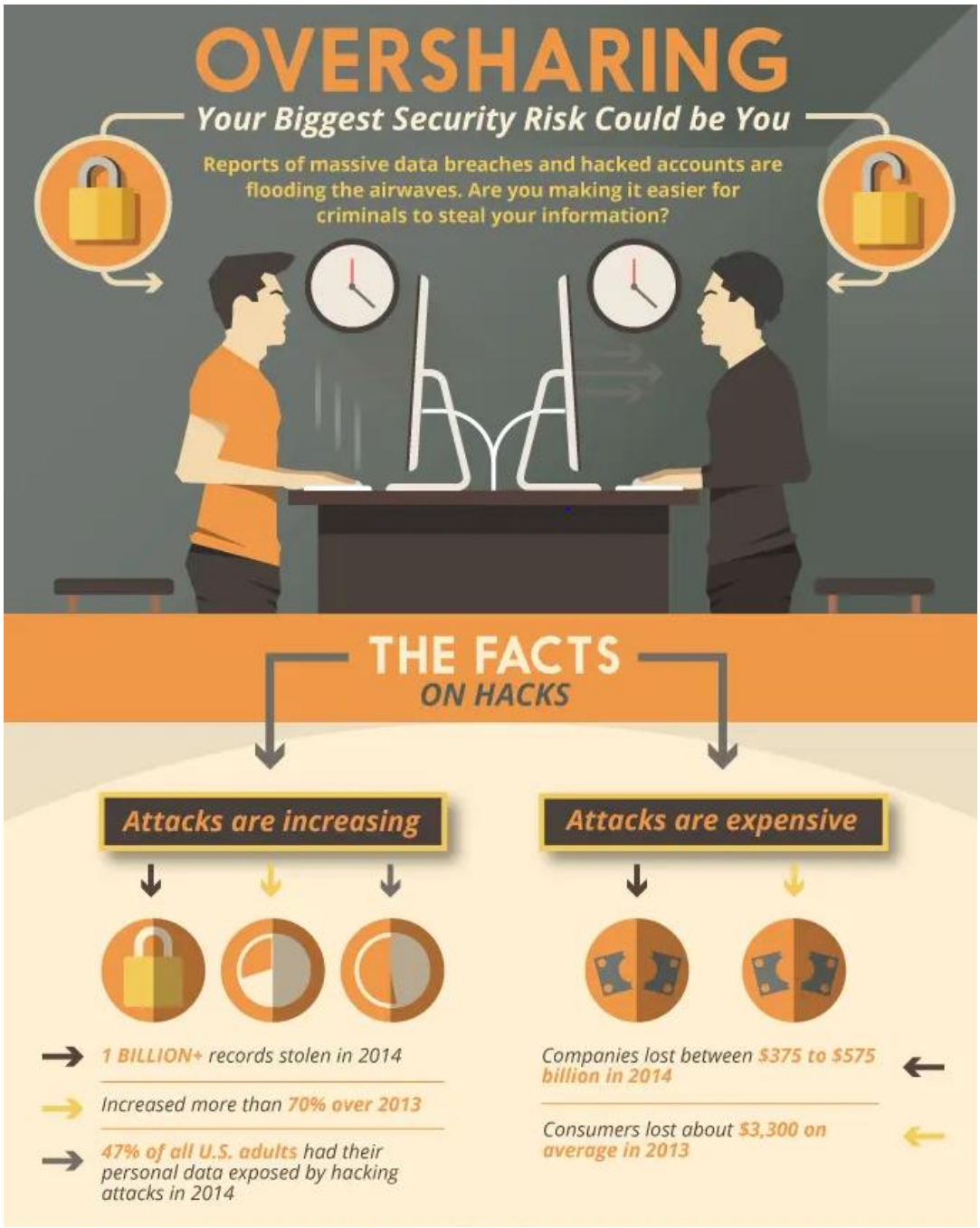
- You can only take photos or videos in the workplace for lawful and work-related purposes.
- You can post, publish or distribute photos or videos taken in the workplace with our permission or if it's for a lawful work-related purpose.

Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance. Civil, criminal, and equitable remedies may apply.

Annual Review

This document will be reviewed and updated by management on an annual basis or when relevant to include newly developed standards into the policy and distribute it to all employees and contracts as applicable.


OVERSHARING
Your Biggest Security Risk Could be You
Reports of massive data breaches and hacked accounts are flooding the airwaves. Are you making it easier for criminals to steal your information?
THE FACTS
ON HACKS
Attacks are increasing
1 BILLION+ records stolen in 2014
Increased more than 70% over 2013
47% of all U.S. adults had their personal data exposed by hacking attacks in 2014
Attacks are expensive
Companies lost between $375 to $575 billion in 2014
Consumers lost about $3,300 on average in 2013


HOW MUCH OF YOU IS ON SOCIAL MEDIA?
DATA YOU MEAN TO GIVE
PERSONALLY IDENTIFIABLE INFO
→ Your name
→ Birthday
→ Photo
→ Any other distinguishing information
CONTACTS
→ Phone address book
→ Email address book
LOCATION DATA
→ Listed location
→ Tagged location on sites like Instagram and Foursquare
BILLING INFORMATION
→ Address
→ Credit Card Information
EMPLOYMENT DATA
→ Previous and current jobs
→ Current coworkers
DATA YOU DON'T MEAN TO GIVE
GPS LOCATION
→ Wi-fi
→ Bluetooth signal
PHONE INFORMATION
→ Service provider
→ Language
→ Time zone
→ Make and model
→ Operating system
- iOS, Android or Windows
- System updates
→ Battery percentage
SOCIAL MEDIA USAGE HABITS
→ Frequency of use
→ Likes and interests
→ Social network interactions
- Messages
- Photos shared
- Close friends vs. acquaintances
→ Visits to partner websites based on ads
According to a May 2015 survey commissioned by the USA Network,
55% of young people say that if they could start fresh, they wouldn't join social media at all


WHAT CAN HACKERS DO WITH YOUR DATA?
PERSONALIZE SOCIAL ENGINEERING ATTACKS AND SPAM EMAILS
Spear phishing is a highly targeted form of phishing attack that relies on personalization to trick victims
Malware-laced emails don't seem as risky when they refer to people or places that are familiar to you
(e.g. names of friends, coworkers, employers or organizations you belong to)
Attacks can be personalized based on your likes and interests and often appear to be sent from "friends" or coworkers
(IT department, bosses, executives, etc.)
HACK OTHER ACCOUNTS
Use the same password and email to try to access your banking account, email or business accounts to steal data
Send spear phishing emails to your employer or coworkers using your information or accounts
Use information gleaned from social media to guess passwords or answer security questions on other sites (e.g. your dog's name, place of birth, or mother's maiden name)
Reset passwords
EXTORTION
Charge a fee to regain control of your profile
Ransom embarrassing photos or conversations
STEAL YOUR IDENTITY
Use current bank accounts
Open new accounts
Create false identities for criminals


TIPS FOR USING SOCIAL MEDIA SAFELY AND SECURELY
Use unique, complex passwords for every online account you own and change them regularly — especially following announcement of a security breach or account compromise
Weigh your risk before posting or sharing information that could be valuable to cybercriminals
Configure privacy settings for your social profiles to control what kind of information you share with others
Never share sensitive information on social media, including financial information, account credentials, confidential company information, and personal information that could be used to steal your identity or compromise your accounts
Be especially wary of unsolicited contact via social media, particularly from people you don't know
Avoid clicking on suspicious links or content in direct messages or news feeds
Only connect with people that you know and trust in real life