MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Procedures for MBIE staff using social media for verification and investigation purposes to support regulatory compliance and law enforcement work

July 2019

Version 1.1

New Zealand Government

Contents

Overview

1. Purpose

The purpose of this document is to help manage the risks for MBIE staff who gather information through social media for verification and investigation purposes to support regulatory compliance and law enforcement work by providing a process, procedures and guidelines that they can consistently use.

This process takes immediate effect and supersedes all other interim or existing advice.

If you have any questions about this process, please contact the Head of Protective Security in the Corporate Governance and Information Group.

2. Scope

This procedure applies to all MBIE staff that use social media to assist their regulatory, compliance and law enforcement work.

The procedures include relevant information to:

1. Assess the risk of using social media for work purposes
2. Determine the access option for using social media
3. Complete the training for using social media
4. Obtain an approval for using social media
5. Set up systems for using social media.

Further guidance includes:

- Monitoring the use of social media
- How the requirements of the Privacy Act apply to the use of social media
- How to manage Official Information Act requests for details about social media.

3. Exemptions

Where an individual and/or a team is unable to meet the provisions of these procedures, they shall contact the Head of Protective Security in the Corporate Governance and Information Group to discuss an exemption to the procedures and/or an appropriate alternative.

4. Definition of terms

Term	Description
Entity	Any type of business, for example, a company, trust, sole trader or partnership.
False persona	A fictitious name or pseudonym used instead of a person's real name to conceal their identity.
Individual	A single, named person.
Level 1 Open unregistered searching	Accessing social media using a generic search engine where no registration is required.
Level 2 Overt passive membership	Accessing social media by logging into a social media forum or community site using an MBIE account and passively observing individuals (e.g. Facebook).
Level 3 Discreet searching (false persona)	Accessing social media using an account with a false persona and passively viewing information.
Level 4 Discreet active engagement (false persona)	Accessing social media using an account with a false persona and actively engaging with individuals – this is not encouraged in MBIE.
MBIE profile	A social media account set up with an individual's name with an MBIE owned suffix, e.g. firstname.lastname@mbie.govt.nz
Social media	The collective of online communication channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation and wikis are all examples of social media.
Stand-alone computer	Any laptop or desktop computer that can run local applications on its own without needing a connection to the MBIE network. Although it may be connected to a network, it is still a stand-alone computer as long as the network connection is not required for its general use.

Assess risk of using social media and determine access method

1. High-level risks

The use of social media for verification and investigation purposes in support of regulatory compliance and law enforcement work needs to be a considered decision. Information gathered from social media may or may not be valuable and, irrespectively, accessing the information carries risks that must be managed.

At a high level, the risks of using social media to gather information for verification and investigation purposes to support regulatory, compliance and enforcement work may be to:

- the rights of New Zealand's citizens and visitors
- the personal safety of MBIE staff or their family
- the security of MBIE's ICT network
- MBIE's reputation and legal liability
- the work of other agencies – domestically and internationally – should MBIE's activities inadvertently overlap with their activities.

2. Use of personal networks, devices and accounts are prohibited

Risks cannot be managed if staff use personal networks, personal devices or personal accounts for searching social media for verification or investigation purposes; therefore these methods are prohibited.

Staff are required to use MBIE's network, devices or accounts, or stand-alone computers, as agreed as part of the approvals process.

3. Methods of access

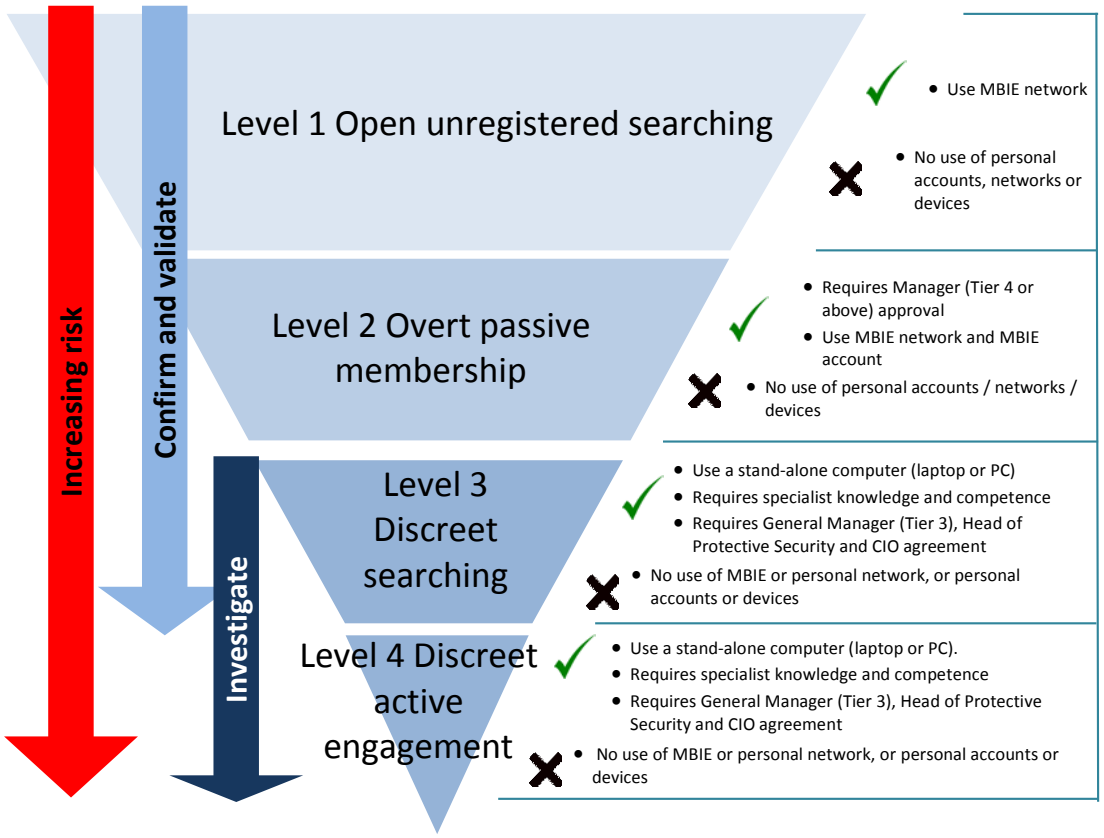
The risks associated with the use of social media vary depending on the method used to access the information. MBIE has identified four methods for accessing information from social media. In order of preferred use, with the most preferred and least risk first, they are:

Method	Purpose	What this looks like
Level 1 Open unregistered searching -no account required -no approval required	To confirm or validate concerns using information that is publicly available and not subject to personalised privacy settings.	Accessing social media information using a generic search engine where no account registration or logging in is required (e.g. searching on a person's name using Google). Is undertaken using MBIE device and network.
Level 2 Overt passive membership -use of @mbie.govt.nz account -approval required	To access and confirm or validate information that may be considered publicly available but is subject to personalised privacy settings that require an account login to view.	Accessing information via social media community membership that requires an account and to be logged in, using an MBIE-profile (@mbie.govt.nz), and only **passively** viewing information. This applies to social media communities like Facebook or LinkedIn and when logged in to search engines like Google Groups.

Level 3 Discreet searching (false persona) -use of false persona account -approval required	To investigate and/or verify a specific individual in relation to a specific task or case, when the risk is mitigated by a false persona to protect the MBIE staff member's identity.	Accessing social media information via community membership, using a standalone device with a false persona that is logged in, and **passively** viewing information.
Level 4 Discreet active engagement (false persona) -use of false persona account -approval required -systems required	To directly engage a specific individual in relation to a specific case, when the risk is mitigated by a false persona to protect the MBIE staff member's identity.	Accessing a social media community with a false persona that is logged in, and **actively engaging** with an individual or forum, using a standalone device that cannot be attributed to either the individual or MBIE.

The diagram below summarises the four access methods and how they are used.

Diagram 1: Accessing information



Confirm access option for using social media

1. Level 1 Open Unregistered Searching

Description

MBIE's preferred search method is to use a generic search engine to gather information from social media on individuals or entities.[1] In practice, this means using the MBIE ICT network and then typing the name of the person or entity directly into Google (or another search engine) and observing only what is returned.

Social Search Engines are another option that allow users to view material without logging in to any specific social media platform, for example:

- Google Social Search www.social-searcher.com/google-social-search

If you are gathering information via social media for the purpose of confirming or validating aspects of a case or decision to be made, this is the recommended approach to take.

Training

All staff using Level 1 Open Unregistered Searching must complete the Social Media for Verification and Investigation – Foundation training course available through Learn@MBIE.

Approval

Level 1 Open Unregistered Searching for work purposes, does not require approval. Essentially this approach is a Google search. Staff do not need permission for non-login searching of the internet. Everyone searches Google and may find social media information, not subject to privacy settings, in this way.

2. Level 2 Overt Passive Membership

This is similar to Level 1 Open Unregistered Searching, except that you are required to register and log in, increasing the risk level. This engagement method should only be used to verify and confirm information and does require management approval.

As soon as you encounter any information that may lead to a formal investigation, you must obtain the appropriate approvals and switch to Level 3 Discreet Searching (false persona) or Level 4 Discreet Active Engagement (false persona).

When registering with the social media site, you must be clearly identified as part of MBIE and so must create and use an MBIE branded profile, i.e. *firstname.lastname@mbie.govt.nz*.

Training

All staff using Level 2 Overt Passive Membership must complete the Social Media for Verification and Investigation – Foundation training course available through Learn@MBIE.

[1] Depending on the privacy settings of the account holder, staff may be able to view all, some, or none of their social media information.

Approval

Level 2 Overt Passive Membership for work purposes must be approved by your Manager (Tier 4 or above). The request and approval should be made by email, using the template at **Appendix 1**, and saved in your branch filing system for future reference.

Approving managers also have discretion to jointly grant permission to undertake Level 2 Overt Passive Membership either at an individual or at a business unit level and on a one off or ongoing basis. Where ongoing approval is granted, this must be reviewed and updated on an annual basis.

3. Level 3 Discreet Searching (false persona)

Level 3 Discreet Searching is used for verification or investigation into matters where grounds for further information gathering have been identified. The decision to transition from Level 2 Overt Passive Membership to Level 3 Discreet Searching will be assessed during the approval process on a case by case basis. Where there is a risk to the staff member or MBIE, , it is recommended Level 3 Discreet Searching using a false persona is used.

Level 3 Discreet Searching is:

- where a stand-alone computer that is not attributable to yourself or MBIE is required
- where a social media account is created as a false persona that leaves no trail back to yourself or MBIE, to protect your identity from others
- where you avoid incorporating any personal information in your false persona profile, including things like date of birth or photographs
- passive – you must not post, like, share, message, join closed groups or friend any of the individuals or entities you are viewing.

Even with passive use, be aware that if you log in to social media and view other people's accounts you may show up in an equivalent of a "Who's viewed your profile" panel (as happens with LinkedIn).

Level 3 Discreet Searching has risks to your personal safety as well as for the security of MBIE's ICT network. For these reasons, a standalone and false personas device must be used for Level 3 Discreet Searching; the false personas must be carefully established, maintained and replaced, as set out in the Social Media False Persona Guidelines. You will agree the most appropriate option for your work with the Chief Information Officer and Head of Protective Security as part of the approval process.

Training

Those staff that need to access social media using a standalone computer and false persona must complete both the Social Media for Verification and Investigation – Foundation course and the Social Media for Verification and Investigation – Advanced course, available through Learn@MBIE.

Approval

Level 3 Discreet Searching (false persona) for work purposes must be approved using the template at **Appendix 2**, and saved in your branch filing system for future reference.

Your General Manager (Tier 3) will approve any request to undertake Level 3 Discreet Searching, confirming this is appropriate for the business.

The Chief Information Officer will approve the information management approach and the technology tool used to complete the task.

The Head of Protective Security will approve the approach from a security perspective.

Approving managers also have discretion to jointly grant permission to undertake Level 3 Discreet Searching either at an individual or at a business unit level and on a one-off or ongoing basis. Where ongoing approval is granted, this must be reviewed and updated on an annual basis.

4. Level 4 Discreet Active Engagement (false persona)

Level 4 Discreet Active Engagement is where a social media account is used with a false persona to actively engage with an individual, entity or group, including joining a closed group. Level 4 Discreet Active Engagement poses the highest legal and reputational risks. It requires specialist knowledge and expertise, requiring particular competence, and should only be used where there is appropriate cause to investigate using this method. The use of Level 4 Discreet Active Engagement will be assessed on a case by case basis through the approval process.

MBIE does not encourage Level 4 searching using a false persona because the personal and reputational risks increase significantly. If you consider Level 4 Discreet Active Engagement is necessary, then your manager must consult with their General Manager (Tier 3), the Head of Protective Security and the Chief Information Officer to determine next steps.

You must set up a new social media account under a false persona for each investigation that requires discreet active engagement. A single social media account must not be used across more than one investigation, to avoid compromising either the account or the investigation, as set out in the Social Media False Persona Guidelines.

A stand-alone computer that is not attributable to yourself or MBIE is required. You will agree the most appropriate option for your work with the Chief Information Officer and Manager Protective Security as part of the approval process.

Training

Those staff that need to access social media using a false persona must complete both the Social Media for Verification and Investigation – Foundation course and the Social Media for Verification and Investigation – Advanced course, available through Learn@MBIE.

Approval

Level 4 Discreet Active Engagement (false persona) for work purposes must be approved using the template at **Appendix 2**, and saved in your branch filing system for future reference.

Your General Manager (Tier 3) will approve any request to undertake discreet active engagement, confirming this is appropriate for the business.

The Chief Information Officer will approve the information management approach and the technology tool used to complete the task.

The Head of Protective Security will approve the approach from a security perspective.

Approving managers also have discretion to jointly grant permission to undertake discreet active engagement either at an individual or at a business unit level and on a one-off or ongoing basis. Where ongoing approval is granted, this must be reviewed and updated on an annual basis.

Complete training for using social media

1. Foundation course

All staff using social media must complete the Social Media for Verification and Investigation – Foundation course before requesting approval to access and use information from social media.

The Foundation course is available through Learn@MBIE.

2. Advanced course

Those staff that need to conduct Level 3 and Level 4 social media searching using a false persona must also complete the Social Media for Verification and Investigation – Advanced course (or equivalent). Any equivalent course will be established by the Head of Protective Security.

The Advanced course is available through Learn@MBIE.

Obtain approval for using social media

1. Approval form

All requests to access and use information from social media must be submitted using the appropriate template. See Appendices 1 and 2.

All approval forms must be saved in the branch filing system.

2. Individual or group approval

All staff using social media must gain appropriate approval for the access option they use. Approval to use social media for work purposes will usually be given on an individual, case-by-case basis.

Where the use of social media is a constant part of a business unit's work, approving managers will have discretion to grant ongoing permission to undertake information gathering via social media at a business unit level.

3. Approval for MBIE staff working overseas

MBIE staff working off-shore will follow the same approval processes as other staff, with additional approval steps from the Operations Manager, Risk Manager and Area Manager.

The Risk Manager is required to assess the social media request to determine if there are any local factors that pose an additional risk to MBIE. Local factors can include legal, operational or security factors.

The Risk Manager is responsible for obtaining local advice on the legality of the request. If legal advice has been provided previously for a similar request, then the Risk Manager can take that into account rather than obtaining additional local legal advice. The Risk Manager and their local legal advisor will consult with MBIE Legal New Zealand, where necessary, to clarify any legal risks or concerns.

4. Approvers' roles and responsibilities

The approval roles and responsibilities are summarised in the following table.

Role	Responsibilities
Chief Security Officer (CSO)	Approve the process and procedures for MBIE staff using social media for verification and investigation purposes to support regulatory, compliance and enforcement work.
Protective Security Requirements (PSR) Governance Committee	Review the process and procedures, and recommend changes and / or acceptance to the CSO.
Managers (Tier 4)	Approve requests to use Level 2 Overt Passive Membership of social media for verification and investigation purposes. Review approvals for use of social media on an annual basis.
General Managers (Tier 3)	Responsible for health, safety and security of their staff. Approve requests to use Level 3 Discreet Searching and Level 4 Discreet Active Engagement of social media for verification and investigation purposes. Review approvals for use of social media on an annual basis.
Chief Information Officer(CIO)	Approve use of technology that provides a safe platform for discreet searching and discreet active engagement use of social media for verification and investigation purposes. Ensure information management is safe and appropriate.
Head of Protective Security	Approve that the approach to Level 3 Discreet Searching and Level 4 Discreet Active Engagement use of social media, for verification and investigation purposes, is appropriately secure. Responsible for the maintenance of the process and procedures. Review approvals for use of social media on an annual basis.
All Managers	Ensure all staff using social media for verification and investigation purposes have undertaken the appropriate training and complete the appropriate registers of use.
All Staff	Ensure the use of social media for verification and investigation purposes is undertaken in an appropriate manner and in accordance with these procedures.
Off-shore Risk, Operations and Area Manager	Approve requests for off-shore use of social media. Determines if there are any local factors that pose an additional risk to MBIE.
Security and Emergency Management Team	The Security and Emergency Management Team is responsible for the central register – a summary of the individual unit registers and maintain a register of approvals

Legal team	Providing advice to teams on the lawfulness of information gathering from social media, including in relation to the Privacy Act 1993 and the Bill of Rights Act 1990 Assisting Risk Managers instruct offshore legal counsel.

5. Approval costs

Approving the request for use of social media confirms the business manager agrees to fund the necessary training, systems or equipment required to enable their staff to use social media in a safe and secure manner for work purposes.

Set up systems for using social media

1. Establishment, maintenance and termination of false persona

The False Persona Guidelines must be used to set up, maintain and terminate false personas to be used for Level 3 Discreet Searching (false persona) and Level 4 Discreet Active Engagement (false persona). Where a team is a high user of social media for verification and investigation purposes, it may be appropriate to set up and maintain a suite of false personas.

2. Register of accounts and use of social media

Each unit of a branch using social media must maintain a register of use, using the Social Media Usage Register template on the Protective Security Policy Pro page, and save it in their unit filing system. The register must be updated when social media is used for verification and investigation purposes in support of regulatory compliance and law enforcement work. If you wish to change the structure of the Usage Register, this must be agreed with the Security and Emergency Management Team.

Where a social media request is declined, the declined request and reason for the decline is to be logged in the decline table.

A central register will be maintained by the Security and Emergency Management Team. A copy of the unit register must be sent to the Security and Emergency Management Team each month at socialmedia.registries@mbie.govt.nz. The central register will provide a summary of the use of Level 3 Discreet Searching (false persona) and Level 4 Discreet Active Engagement (false persona) and allow oversight of the use of social media within MBIE.

3. How to manage the collection and storage of evidence

The collection and storage of information will be managed as agreed in the approval process. This will usually involve taking screenshots and saving them into Word documents. These documents need to be saved within an appropriately secure filing structure. The information collected should be noted in the register.

4. Equipment required for use of social media

Level 3 Discreet Searching and Level 4 Discreet Active Engagement (false persona) use of social media requires the use of a stand-alone computer that is not attributable to staff or MBIE. You will agree the most appropriate option for your work with the Chief Information Officer and Head of Protective Security as part of the approvals process.

Monitoring the use of social media

It is important to understand how MBIE's use of social media for regulatory compliance and law enforcement purposes responds to the changes in the use of social media, while ensuring the procedures are fit for purpose now and in the future as new social media platforms arise.

The use of social media across MBIE will be monitored by the Security and Emergency Management Team to gather information on the use, benefits, costs and issues of using social media as set out in these procedures. The monitoring will be used to refine the procedures and ensure staff are operating within the process to keep themselves safe online. Monitoring will include the:

- branch/units using social media
- use of social media access options
- use of social media sites
- value of the information gathered through social media for verification and investigation work, including number and type of cases
- number of staff completing social media training and the cost of it
- suitability and cost of equipment
- compliance by staff with the social media procedure.

A quarterly report will be produced to the Protective Security Requirements (PSR) Governance Committee.

The Privacy Act and the use of social media

Information posted on social media is subject to the Privacy Act 1993 if the information is about an individual. The main requirements are that:

- the collection of the information is necessary for a lawful purpose connected to the function of the agency
- information is collected lawfully and fairly and in a manner that does not unreasonably intrude on the individual
- information is accurate, up to date, complete, relevant, and not misleading, and where possible corroborated
- information is held and transferred safely and securely
- information is only used and shared for the reasons it has been collected.

Staff using Level 2 Overt Passive Membership, Level 3 Discreet Searching and Level 4 Discreet Active Engagement methods to access and collect information through social media for verification and investigation purposes to support regulatory compliance and law enforcement work, must comply with the requirements of the Privacy Act 1993.

To evidence compliance with the Privacy Act, staff must produce a plan within their approval request that demonstrates why social media is being used and how it will be used. This plan must clearly document what staff intend to do, what they have considered and what training they have undertaken. Staff should use the appropriate approval template to do this, and ensure that they complete the Social Media Usage Register.

Official Information Act requests for details about social media

Any Official Information (OIA) Act request for details about social media information held about an individual is managed using the usual OIA process.

To respond to a request, if no withholding grounds apply, details may be pulled from the Social Media Usage Register and agreed approach as given in the approval documents.

Care will need to be taken to balance individuals' privacy, and prejudice to the maintenance of the law, with the public interest.

Appendix 1: Template for approval of Level 2 Overt Passive Membership for an individual or business unit

<table>
<tr><th colspan="3">Request to access and use information from social media – LEVEL 2 OVERT PASSIVE MEMBERSHIP</th></tr>
<tr><td colspan="2">Details of staff member(s) requesting to use social media for work purposes</td><td>Name, position, unit and group.

Include whether the request is at individual or business unit level and whether it is for a one off or ongoing use.</td></tr>
<tr><td colspan="2">Rationale for accessing and using social media</td><td>This section must include the valid and lawful reason for accessing social media – the specifics on what the information is intended to assist with – the purpose.</td></tr>
<tr><td colspan="2">Plan for collecting information from social media</td><td>The plan must describe:
• how the staff member will record their social media search activities.
• how the staff member will ensure that only information relevant to the purpose is collected.
• how information from social media will be verified using other sources.
• how the rights of the public in relation to searches by the State are considered and protected.</td></tr>
<tr><td colspan="2">Where and how the information will be safely and securely stored</td><td>For example: Capture a screen shot of the relevant material and then crop or obscure the top and sides of the frame to ensure that the account identity used to gather the information is not revealed. Ensure that the information is named with the access date.

Provide directions to where the information will be securely stored, including who has access rights and directions to the unit’s Social Media Usage Register.</td></tr>
<tr><td colspan="2">Competence</td><td>Confirmation that all staff members to whom this approval relates have completed the Use of Social Media for Verification and Investigation – Foundation training course.</td></tr>
<tr><td rowspan="3">These three approvals only completed for off-shore requests</td><td>Head of Operations review (as available)</td><td>This may be a physical signature or embedded email with agreement to this plan</td></tr>
<tr><td>Risk and Verification Manager assessment (as available)</td><td>Details the outcome of the risk assessment and whether there are any local factors that pose an additional risk to MBIE. Local factors can include legal, operational, or security factors.

Risk and Verification Manager notes whether local legal advice has been obtained and when it was obtained.</td></tr>
<tr><td>AGM approval (as available)</td><td>This may be a physical signature or embedded email with agreement to this plan and acceptance of the risk assessment.</td></tr>
<tr><td colspan="2">Manager (Tier 4 or above) approval</td><td>This may be a physical signature or embedded email with agreement to this plan, date of approval and a date for review (usually annual).</td></tr>
</table>

Appendix 2: Template for approval of discreet searching or discreet active engagement for an individual or business unit

Request to access and use information from social media – LEVEL 3 DISCREET SEARCHING & LEVEL $ DISCREET ACTIVE ENGAGEMENT		
Details of staff member(s) requesting to use social media for work purposes		Name, position, unit and group. Include whether the request is at individual or business unit level and whether it is for a one off or ongoing use.
Rationale for accessing and using social media		This section must include the valid and lawful reason for accessing social media – the specifics on what the information is intended to assist with – the purpose.
Plan for collecting information from social media		The plan must describe: • what systems and tools will be used to safely access social media • how the staff member will record their social media search activities • how the staff member will ensure that only information relevant to the purpose is collected • how information from social media will be verified using other sources • how the rights of the public in relation to searches by the State are considered and protected • how the false persona will be created and what will happen to the false persona at the end of the investigation.
Where and how the information will be safely and securely stored		For example: Capture a screen shot of the relevant material and then crop or obscure the top and sides of the frame to ensure that the account identity used to gather the information is not revealed. Ensure that the information is named with the access date. Provide a link to where the information will be securely stored, including who has access rights and directions to the unit's Social Media Usage Register.
Competence		Confirmation that all staff members to whom this approval relates have completed both the Use of Social Media for Verification and Investigation – Foundation training course and the Use of Social Media for Verification and Investigation – Advanced training course (or equivalent).
These three approvals only completed for off-shore requests	**Head of Operations review (as available)**	This may be a physical signature or embedded email with agreement to this plan.
	Risk and Verification Manager assessment (as available)	Details the outcome of the risk assessment and whether there are any local factors that pose an additional risk to MBIE. Local factors can include legal, operational or security factors. Risk and Verification Manager notes whether local legal advice has been obtained and when it was obtained.
	AGM approval	This may be a physical signature or embedded email with agreement to this plan

	(as available)	and acceptance of the risk assessment.
General Manager (Tier 3) approval		This may be physical signature or embedded email with agreement to this plan.
Chief Information Officer approval		This may be physical signature or embedded email with agreement to this plan.
Head of Protective Security approval		This may be physical signature or embedded email with agreement to this plan.

Appendix 3: Social Media Usage Registers

IN CONFIDENCE

Social Media Information Gathering Record of Use - Level 2

ALL cells must be filled out
(unless you have a pre-approved exemption - contact socialmedia.registries@mbie.govt.nz for queries)

Search Number	Business Unit	Access Search Level	Staff Member Accessing	Date and Time of Access	Mission/ Case ID	Person/ Entity of Interest Name	Reason for Search	Was Reason for Search Met	Names of Websites Searched EG. Facebook, Instagram, Google	Was information captured	Information Storage Location	Notes
1	Enterprise Risk and Assurance	L2 Overt Passive Membership	Jane Smith	10:00am 01/04/19	7032	Adam Johnson	Verification	Yes	Google Custom Search Facebook	Yes	MAKO	NA
2												
3												

IN CONFIDENCE

Social Media Information Gathering Record of Use - Level 3 & Level 4

ALL cells must be filled out
(unless you have a pre-approved exemption - contact socialmedia.registries@mbie.govt.nz for queries)

Search Number	Business Unit	Access Search Level	Staff Member Accessing	Date and Time of Access	False Persona Name Fill in Persona Library first	Mission/ Case ID	Person/ Entity of Interest Name	Reason for Search	Was Reason for Search Met	Names of Websites Searched EG. Facebook, Instagram, Google	Was information captured	Information Storage Location	Notes
1	Enterprise Risk & Assurance	L3 Discreet Searching	Janet Smith	10:00am 01/04/2019	Abbey Jerard	7032	Adam Johnson	Verification	Yes	Facebook Instagram LinkedIn	Yes	MAKO	NA
2													
3													

IN CONFIDENCE

False Persona Library

Link to the False Persona Guidelines

All cells must be filled out
The layout below follows the False Persona Guidelines

Record Management							*Part 1: Create a false name, date of birth and password*					*Part 2: False Email Accounts*		*Part 3: Social media accounts*		*Other*
Persona Number	Business Unit	Employee Who is Creating	Date Activated	Date Retired NA if still active	Retired Reason Select "Still Active" if not	Retired by who NA if still active	Persona Nationality	Persona Name	Is this a name of a MBIE worker? Check on the Link	Date of Birth	Persona Password To be used for accessing all sites	Email Address for Social Media	Email Address for Communicating to MBIE	All Social Media Profiles Use "Alt + Enter" to add multiple lines	Cell Phone Number NA if none	Persona Notes Any relevant information including security access questions
1	Enterprise Risk & Assurance	Janet Smith	1/04/2019	NA	Still Active	NA	Australian	Abbey Jerard	No	25/02/1985	Hello@Abbey	Abbey.Jerard@gmail.com	swift2019@gmail.com	Facebook Instagram LinkedIn	6421555055	NA
2																
3																

IN CONFIDENCE

Social Media Information Gathering Record of Use - Decline Register

Employee Name	Work Branch/ Unit	Social Media Trigger Reason for Access	Reason for Decline	Date Declined

Appendix 4: Supporting documents

Mandatory internal documents

- MBIE Code of Conduct
- Information Gathering for Regulatory Compliance, Law Enforcement and Protective Security Policy
- Protective Security Policy
- ICT Acceptable Use Policy
- Records Management Policy
- Use of Social Media for Verification and Investigation Purposes – Factsheet
- Use of Social Media for Verification and Investigation Purposes – Approval Forms [no current hyperlink]
- Use of Social Media for Verification and Investigation Purposes – False Persona Guide
- Use of Social Media for Verification and Investigation Purposes – Standalone Laptop Guide
- Social Media Information Gathering Record of Use – Level 2 [no current hyperlink]
- Social Media Information Gathering Record of Use – Level 3 & Level 4 [no current hyperlink]

Legislation

- Health and Safety at Work Act 2015
- Information Gathering and Public Trust
- Official Information Act 1982
- Privacy Act 1993
- Protective Security Requirements (PSR)
- Public Records Act 2005
- Search and Surveillance Act 2012
- State Services Standards of Integrity and Conduct (SSC Code of Conduct)
- The Bill of Rights Act 1990