NEW ZEALAND
CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA
PROTECTING NEW ZEALAND'S BORDER

WELLINGTON
The Customhouse, 1 Hinemoa Street, Wellington
PO Box 2218, Wellington 6140
Phone: 04 901 4500 Fax: 04 901 4555 All general enquiries phone: 0800 428 786
Email: feedback@customs.govt.nz Website: www.customs.govt.nz

30 June 2022 Ref: OIA 22-085

[redacted]

By email: [redacted]

Tēnā koe [redacted]

Request for information under the Official Information Act 1982

Thank you for your email dated 24 May 2022 to the New Zealand Customs Service (Customs), in which you request the following under the Official Information Act 1982 (the Act):

1. *The number of reports of integrity breaches by Customs staff in each of the years 2017, 2018, 2019, 2020, 2021 and 2022 to date;*

2. *The number of upheld integrity breaches by Customs staff in each of the years 2017, 2018, 2019, 2020, 2021 and 2022 to date, also broken down by the type of integrity breach.*

3. *A more detailed overview of each of the upheld integrity breaches in 2020, 2021 and 2022 to date, including the circumstances and location of the breach and what action was taken in response;*

4. *All reports and briefings regarding and/or discussing the threat of organised crime to staff integrity within Customs;*

5. *The number of Customs staff currently on special leave after integrity complaints.*

Question one and two

> *The number of reports of integrity breaches by Customs staff in each of the years 2017, 2018, 2019, 2020, 2021 and 2022 to date;*
>
> *The number of upheld integrity breaches by Customs staff in each of the years 2017, 2018, 2019, 2020, 2021 and 2022 to date, also broken down by the type of integrity breach.*

In response to question one and two of your request, I refer you to an attached document titled *"Appendix one - The number of reports of integrity breaches and upheld integrity breaches by Customs staff"* providing you with the number of reports of integrity breaches by Customs staff and the number of upheld integrity breaches by Customs staff broken down by type of integrity breaches in each of the financial years 2017, 2018, 2019, 2020, 2021 and 2022 to date.

Question three

> *A more detailed overview of each of the upheld integrity breaches in 2020, 2021 and 2022 to date, including the circumstances and location of the breach and what action was taken in response;*

Customs has considered question three of your request and has concluded that providing details of a breach with a detailed overview, including circumstances and location, would present a very high risk of being able to identify the individuals concerned, both the respondent and the complainant. Therefore, this part of your request is refused under Section 9(2)(a) of the Act to protect the privacy of natural persons.

Customs has considered the public interest arguments in favour of making this information available, however, it is considered that these interests do not outweigh the necessity to withhold the information.

Question four

> *All reports and briefings regarding and/or discussing the threat of organised crime to staff integrity within Customs;*

In response, Customs has identified two PowerPoint presentations in scope, regarding the threat of organised crime to staff integrity within Customs. I refer you to an attached document titled *"Appendix two - presentations discussing the threat of organised crime"* which contains two PowerPoint presentations titled *"Security at Customs 21 Feb 22 ITO"* and *"(Updated) Cohort Integrity workshop Feb 2022"*. These presentations are routinely used in the staff training context for both cohorts and other work groups as and when required.

Question five

> *The number of Customs staff currently on special leave after integrity complaints.*

As at 24 May 2022, there are no Customs staff currently on special leave or on suspension as a result of an integrity complaint.

You have the right, by way of complaint to the Office of the Ombudsman under section 28(3) of the Act, to seek an investigation and review of this response. Information about how to make a complaint is available online at: www.ombudsman.parliament.nz, or you can phone 0800 802 602.

If you have any queries about this response, please contact Prasheeta Ram-Taki, Communications and Media Manager in the first instance on 029 357 0310 or Prasheeta.Ram-Taki@customs.govt.nz .

Please note that Customs may proactively release the response to your Official Information Act request on our website – however, we would not do so for at least two months and your name and contact details would be removed.

Nāku noa, nā

[redacted]

Janine Foster
Director Risk, Security and Assurance

Appendix one: Number of reports of integrity breaches and upheld integrity breaches by Customs staff in each of the years 2017, 2018, 2019, 2020, 2021 and 2022 to date

OIA 22-085 [redacted]

2017/18: The following table shows the outcomes of the investigations into allegations of unacceptable behaviour by Customs staff and contractors/consultants engaged by Customs that were concluded in the 2017/18 financial year:

Upheld	Not upheld	Withdrawn	Person left Customs	Did not meet the threshold of misconduct
11	4	3	4	5

Where misconduct or serious misconduct was found, the particular types of unacceptable behaviour alleged are shown in the following table:

Type of unacceptable behaviour alleged	Upheld	Not Upheld
Actions which bring the Service into disrepute	1	-
Inappropriate use of, or access to, Customs systems	5	-
Inappropriate behaviour at work	2	1
Knowingly making a false declaration	1	-
Conflict of interest	1	1
Attendance	1	1
Failure to follow procedures	-	1
TOTAL	**11**	**4**

When misconduct occurs and it is determined that disciplinary measures are necessary, these are meant to be corrective in nature rather than punitive. In some cases termination is justified and appropriate. The following table provides statistics on disciplinary action or sanctions during the 2017/18 financial year.

Formal warning[1]	Termination (with or without notice)
10	1

The one termination during the 2017/18 financial year related to an employee who made a false declaration.

Of the 10 warnings issued, six were classified as final written warnings.

[1] A formal warning could also include one or a combination of the following: referral to Employee Assistance Programme or other professional assistance; removal of delegated powers; removal of privileges; transfer; demotion; non-eligibility for merit remuneration increase or one-off payment; change of reporting time or hours of work; or such other penalty decided by the Chief Executive.

2018/19: *The following table shows the outcomes of the investigations concluded in 2018/19 into allegations of unacceptable behaviour by Customs staff and consultants engaged by Customs.*

Upheld	Not upheld	Withdrawn	Person left Customs*	Did not meet the threshold of misconduct
14	3	0	1	5

*The employee or contractor/consultant left Customs before the investigation was concluded

Where the threshold for misconduct was met, the types of unacceptable behaviour alleged are shown in the following table:

Type of unacceptable behaviour alleged	Upheld	Not upheld
Actions or behaviour which did (or had the potential to) bring Customs into disrepute	1	–
Inappropriate use of, or access to, Customs systems	2	–
Inappropriate behaviour at work	7	–
Knowingly making a false declaration/dishonesty	1	–
Inappropriate behaviour outside of work	–	1
Misuse of leave/attendance issue	1	–
Misuse of drugs	1	1
Failure to follow correct procedures	1	1
Total	**14**	**3**

When misconduct occurs and it is determined that disciplinary measures are necessary, these measures are meant to be corrective rather than punitive. In some cases termination is justified and appropriate. The following table provides statistics on disciplinary action or sanctions during the 2018/19 financial year.

Formal warning[2]	Termination (with or without notice)
11	1

The one termination during the 2018/19 financial year related to the use of illegal drugs by an employee. Of the 11 formal warnings issued, one was classified as a final written warning and the remaining 10 were first written warnings. In the context of a workforce of over 1,300 employees, these numbers are not statistically significant, and have not increased year-on-year.

Customs records all this information, giving us the opportunity to identify issues, trends, and lessons, and enabling the Customs Executive Board and our Assurance and Risk Committee to consider broader integrity, ethical, or cultural matters.

[2] A formal warning could also include one or a combination of the following: referral to Employee Assistance Programme or other professional assistance; removal of delegated powers; removal of privileges; transfer; demotion; non-eligibility for merit remuneration increase or one-off payment; change of reporting time or hours of work; or such other penalty decided by the Chief Executive

2019/20: *The following table shows the outcomes of investigations concluded in 2019/20 into allegations of unacceptable behaviour by Customs staff and contractors/consultants we engaged.*

Type of unacceptable behaviour alleged	Upheld	Not upheld	Did not meet threshold for misconduct	Person left Customs*	Total
Inappropriate behaviour at work	7	4	5	1	17
Inappropriate behaviour outside of work	3	1	1	–	5
Inappropriate use of, or access to, Customs systems	1	2	–	–	3
Conflict of interest	1	1	–	–	2
Bullying	–	2	–	–	2
Actions or behaviour which did (or had the potential to) bring Customs into disrepute	2	–	–	–	2
Misuse of drugs	1	–	–	–	1
Failure to follow correct procedures	–	1	–	–	1
Performance	1	–	–	–	1
TOTAL	**16**	**11**	**6**	**1**	**34**

When misconduct occurs and it is determined that disciplinary measures are necessary, these measures are meant to be corrective rather than punitive. In some cases termination is justified and appropriate. The following table provides statistics on disciplinary action, sanction, or outcome during the 2019/20 financial year, where the allegation was upheld.

Formal warning[3]	Letter of expectation	Termination (with or without notice)	Resignation	Other
9	3	1*	2	1

*The employee or contractor/consultant left Customs before the investigation was concluded

The one termination during the 2019/20 financial year related to a serious conflict of interest. One resignation related to a penultimate finding of serious misconduct for drug use. In the second instance the individual resigned following a finding of substance to the allegations but prior to a disciplinary outcome being determined. The "Other" relates to substance being found regarding an allegation but where no respondent had been identified.

Of the nine formal warnings issued, two were classified as verbal warnings, three were first written warnings and the remaining four were final written warnings. In the context of a workforce of over 1,500 employees, these numbers are not statistically significant.

[3] A formal warning could also include one or a combination of the following: referral to Employee Assistance Programme or other professional assistance; removal of delegated powers; removal of privileges; transfer; demotion; non-eligibility for merit remuneration increase or one-off payment; change of reporting time or hours of work; or such other penalty decided by the Chief Executive.

2020/21: *The table below shows the outcomes of investigations concluded in 2020/21 into allegations of unacceptable behaviour by our staff and contractors/consultants.*

Upheld	Not upheld	Person left Customs*	Did not meet the threshold of misconduct
11	11	1	-

*The employee or contractor/consultant left Customs before the investigation was concluded. Included in Not Upheld

When misconduct occurs and it is determined that disciplinary measures are necessary, these measures are meant to be corrective rather than punitive. In some cases termination is justified and appropriate.

The table below shows statistics on disciplinary action, sanction or outcome during the 2020/21 financial year, where the allegation was upheld.

Formal warning	Letter of expectation	Termination (with or without notice)	Resignation	Other
8	4	-	-	2

Three of the formal warnings also included a letter of expectation. The 'Other' incidents regard a seconded employee from another organisation and a situation where there was a one-off breach of process.

Of the eight formal warnings issued, two were classified as verbal warnings, two were first written warnings and the remaining four were final written warnings. In the context of a workforce of over 1,500 employees, these numbers are not statistically significant.

2021/30 May 2022: *The following table shows the outcomes of the investigations concluded in 2021 to May 31 2022 into allegations of unacceptable behaviour by Customs staff and consultants engaged by Customs.*

Type of unacceptable behaviour alleged	Upheld	Not upheld	Did not meet threshold for misconduct	Person left Customs*	Total
Inappropriate behaviour at work	2	2			**4**
Inappropriate behaviour outside of work				1	**1**
Inappropriate use of, or access to, Customs systems	3	1		–	**4**
Conflict of interest				–	
Bullying				–	**–**
Actions or behaviour which did (or had the potential to) bring Customs into disrepute		2			**2**
Misuse of drugs	1				**1**
Failure to follow correct procedures					
Performance					
TOTAL	**6**	**5**		**1**	**12**

Formal warning[4]	Termination (with or without notice)*
3*	-

*Of the 3 warnings issued, two were classified as final written warnings and one as first written warning

[4] A formal warning could also include one or a combination of the following: referral to Employee Assistance Programme or other professional assistance; removal of delegated powers; removal of privileges; transfer; demotion; non-eligibility for merit remuneration increase or one-off payment; change of reporting time or hours of work; or such other penalty decided by the Chief Executive.

Integrity Awareness Workshop

NEW ZEALAND CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

PROTECTING NEW ZEALAND'S BORDER

New Zealand Government

Integrity awareness

Today's session will cover:

- What is Integrity?
- How to speak up if you have concerns
- The consequences of inappropriate behaviour
- What's okay and what's not okay

Raise your hand at any time to ask a question or comment

What is Integrity?

What is Integrity?

- Trust

What is Integrity?

- Trust
- Honesty

What is Integrity?

- Trust
- Honesty
- Professionalism

What is Integrity?

- Trust
- Honesty
- Professionalism
- Reliability

What is Integrity?

- Trust
- Honesty
- Professionalism
- Reliability
- Doing what's right

What is Integrity?

- Trust
- Honesty
- Professionalism
- Reliability
- Doing what's right
- Loyalty

What is Integrity?

- Trust
- Honesty
- Professionalism
- Reliability
- Doing what's right
- Loyalty
- Truthfulness

What is Integrity?

- Trust
- Honesty
- Professionalism
- Reliability
- Doing what's right
- Loyalty
- Truthfulness
- Unbiased

What is Integrity?

- Trust
- Honesty
- Professionalism
- Reliability
- Doing what's right
- Loyalty
- Truthfulness
- Unbiased
- 24/7

What is Integrity?

Living Customs' values, especially *We do what's right (Te Ara Tika)*

Our Code of Conduct sets out expected standards of behaviour:

1. Fair
2. Impartial
3. Responsible
4. Trustworthy

24/7

Maintaining trust and confidence in Customs (both internally & externally)

Conflict of Interest declaration – it's often about perception

Know your Customs' policies

- Code of Conduct
- Conflict of Interest
- Gifts and Hospitality
- Social Media Use
- Use of Customs Systems and Devices
- Alcohol at Work
- Protected Disclosures (Whistleblowing)
- Secondary Employment

How to speak up if you have concerns

It's safe to speak up

Tell someone:

1. Talk to your manager or any senior leader
2. Talk to a HR Advisor
3. Use the internal reporting form: Integrity Matters
4. Email Integrity@Customs.govt.nz
5. Report to our anonymous 24/7 Integrity Line (external service)

0800 835 269

Consequences of inappropriate behaviour

- Notifications of inappropriate behaviour are triaged by the Integrity team and HR
- May trigger an investigation (fact finding) or be referred to an employment matters meeting
- What actually happened?
- Has there been a breach of the Code of Conduct?
- Where misconduct is found or the allegation is upheld, the disciplinary policy sets out the disciplinary process and potential outcomes

Disciplinary process – potential outcomes

Depends on the seriousness of the employee's actions:

- Letter of expectation
- Performance Improvement Plan (PIP)
- Training
- First written warning
- Final (second) written warning
- Dismissal

The Integrity Committee

- Provides oversight of the integrity reporting and response process
- Provides assurance that integrity matters are addressed in a transparent, fair and timely manner
- Meets monthly to discuss trends and identify any improvements
- Chaired by Assistant Commissioner of Police (external representative)
- Other members are from within Customs (internal) representing a range of Customs functions and locations

What's okay and what's not okay

Types of inappropriate behaviour (what's not okay) can include:

- Sharing your access card and/or password with colleagues
- Leaving your screen unlocked when away from your computer
- Deliberate misuse of leave
  (e.g. working a secondary job while on sick leave)
- Having conversations in public about clients or Customs' matters

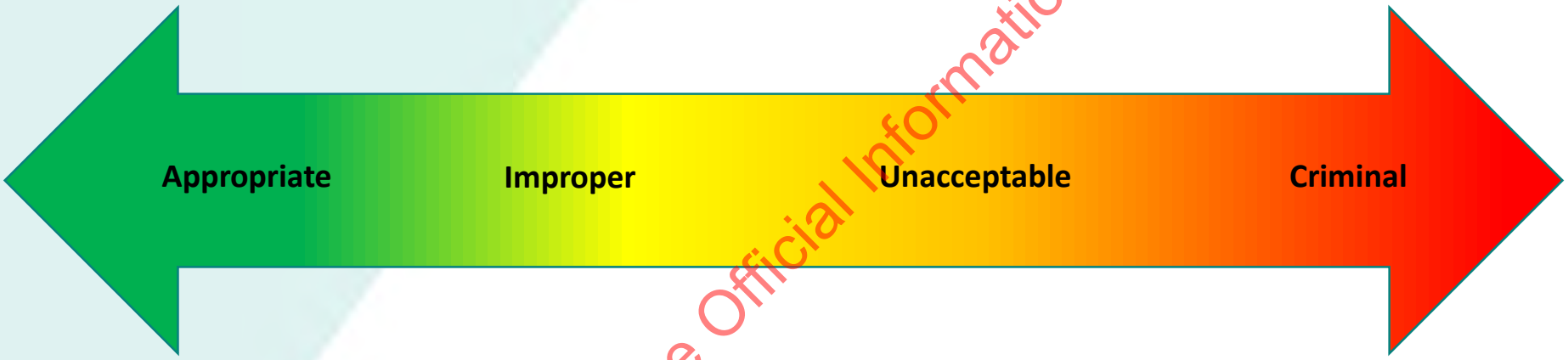
What's okay and what's not okay

- Integrity is not always black and white
- Sometimes there is no obvious right or wrong
- Situations and opinions are generally context specific
- Sometimes there can be mitigating circumstances
- Think about how things might be perceived by others (what impression might they get of you and/or Customs)

Integrity breaches are often a case of poor judgement, people doing dumb stuff.

If you are unsure, ask someone!

INTEGRITY BEHAVIOUR CONTINUUM



Examples:

Appropriate	Improper	Unacceptable	Criminal
Showing dignity and respect to all Treating information with care	Questionable language and jokes Making demeaning comments	Threatening or abusive behaviour directed at others	Offences under Crimes Act or Misuse of Drugs Act

Scenario discussions

Discuss each scenario

- Where does it best fit on the Integrity Continuum and why?
- What about the scenario makes it appropriate/improper /unacceptable/criminal?

Think about:

- What perceptions might arise from the scenario?
- What are the potential consequences?
- How might we address the situation?
- Is there a Customs policy that applies?

Bring back your insights for sharing with the group

Scenario 1

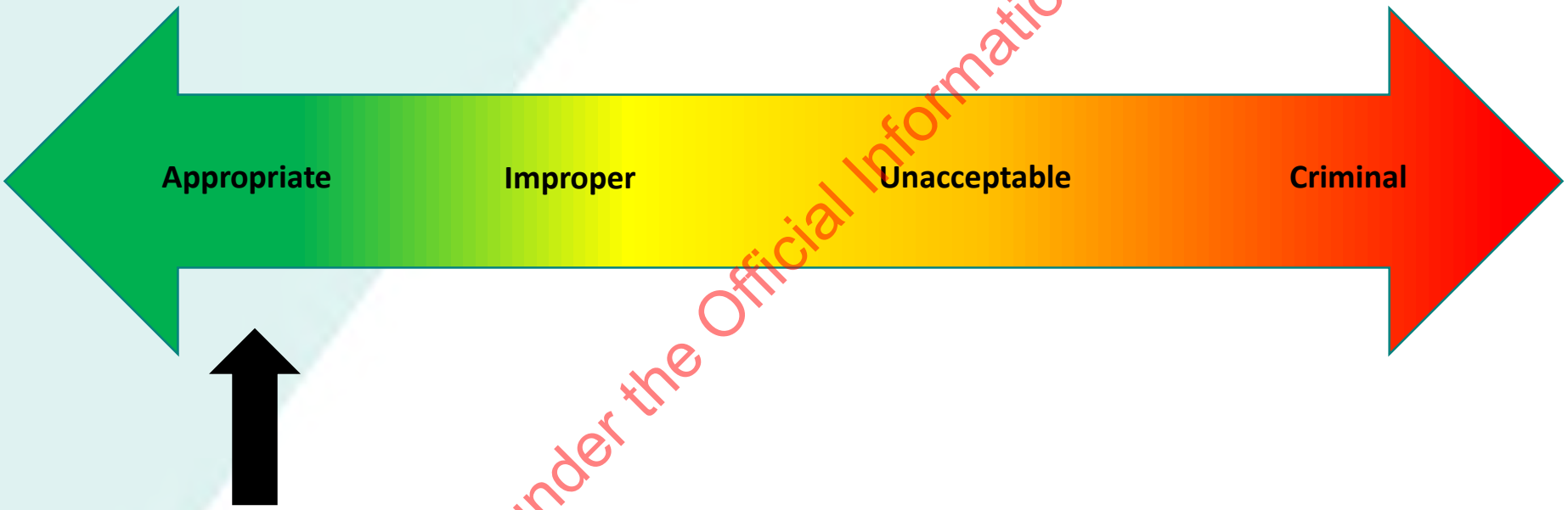
Kasey, a dog handler is asked to visit a local school to talk to students about drug awareness.

At the end of their presentation Kasey is given a $50 book voucher from the school.

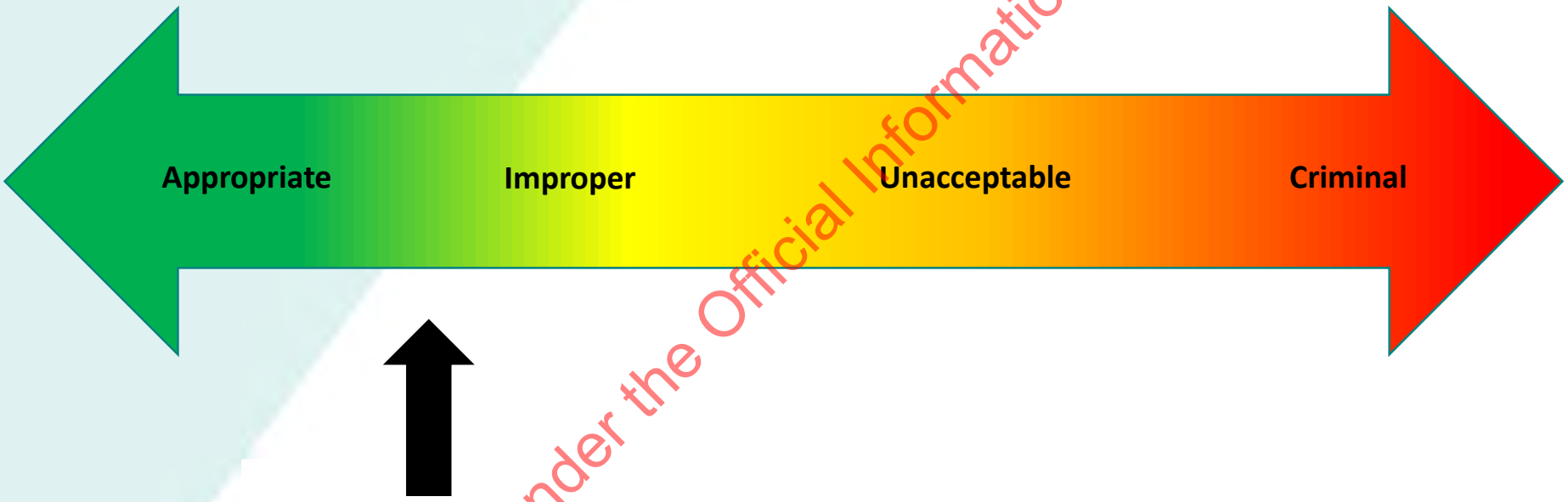
On their return to the office, Kasey passes the voucher on to their Supervising Customs Officer, Sarah.

Sarah returns the voucher to Kasey and tells them to use it.

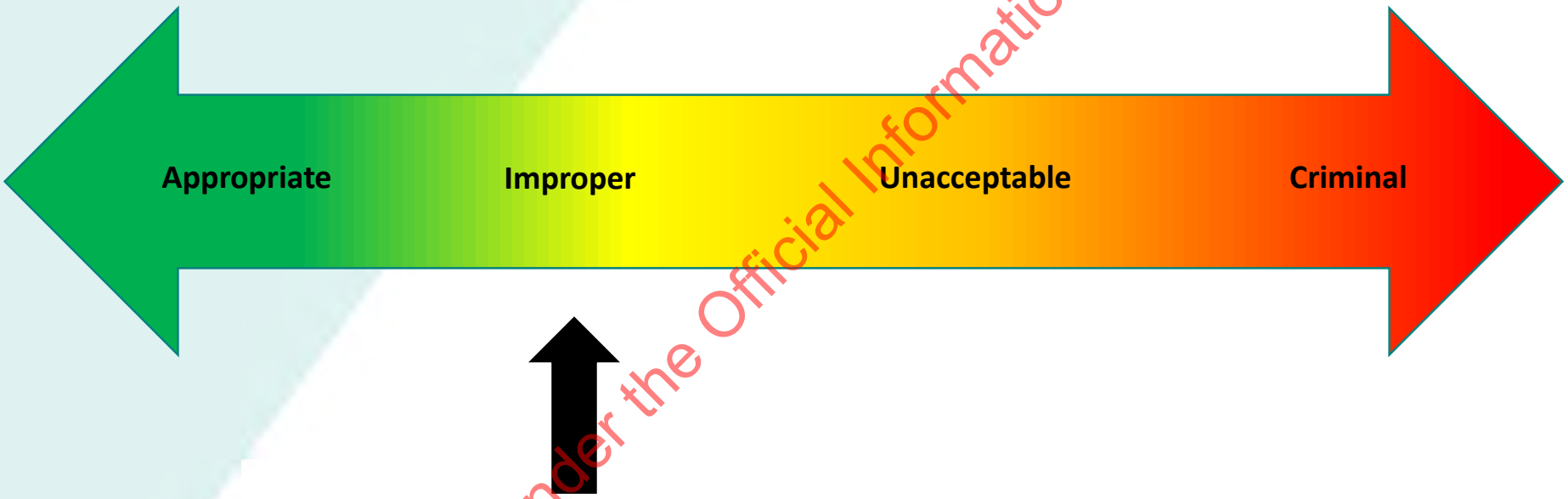
Where does the scenario fit?



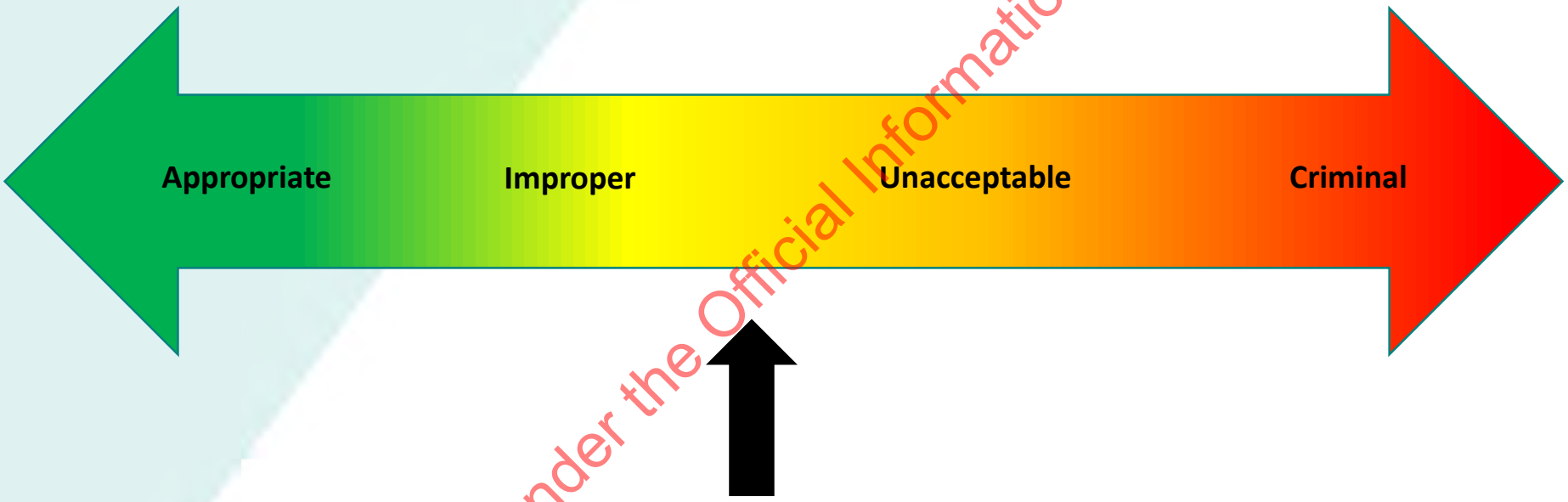
Where does the scenario fit?



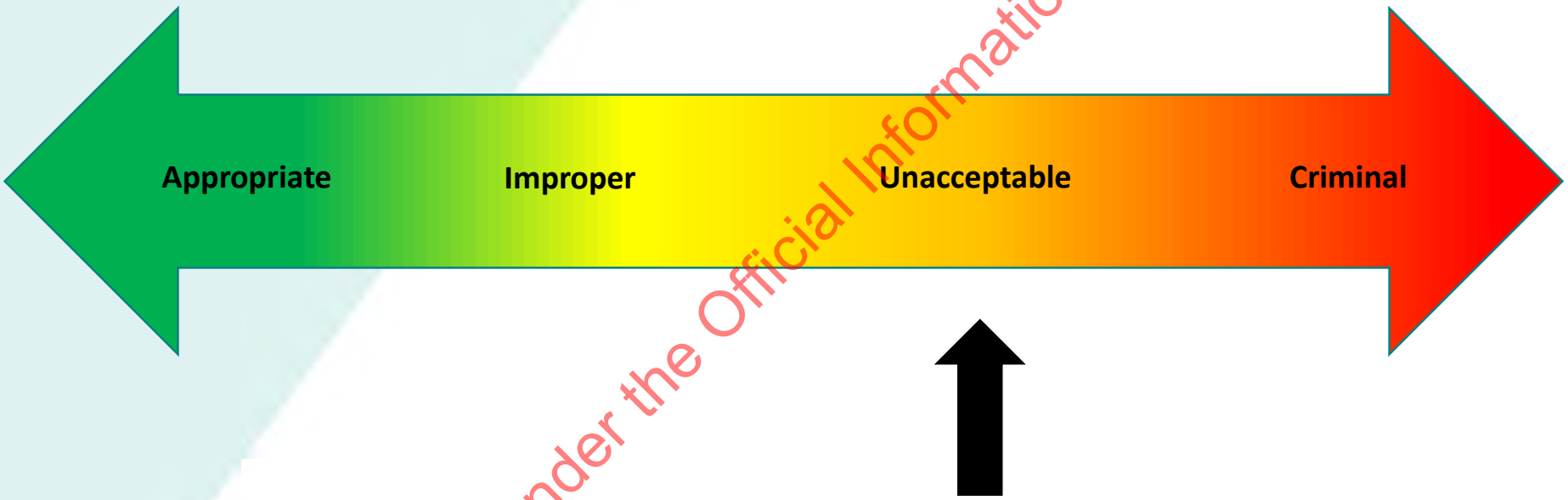
Where does the scenario fit?



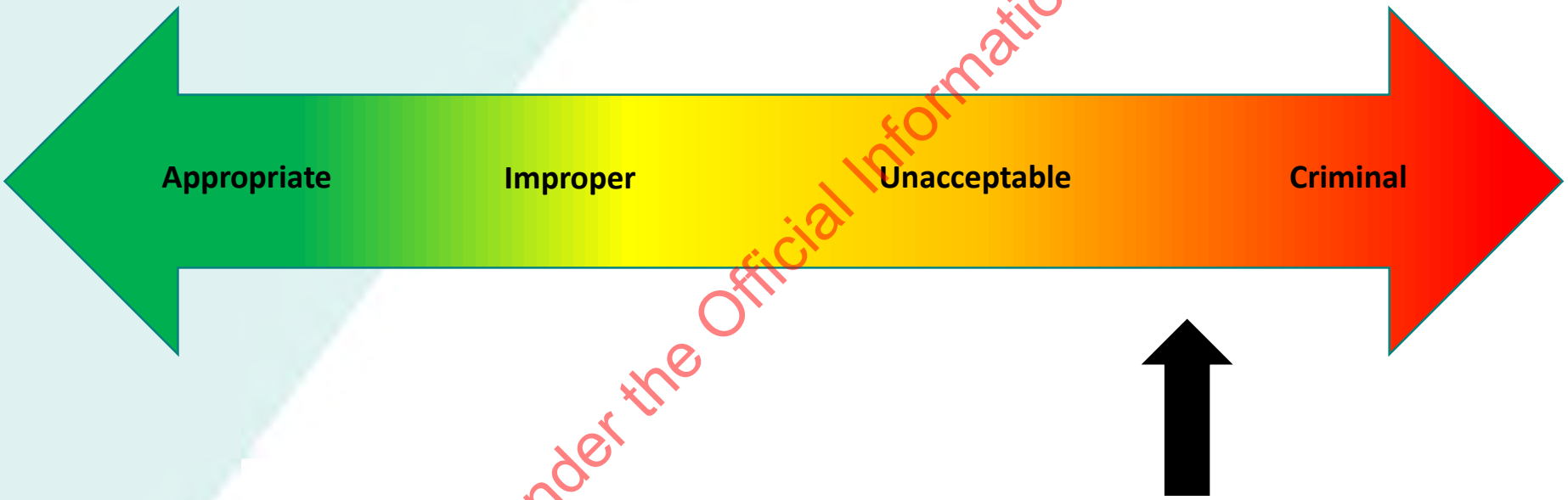
Where does the scenario fit?



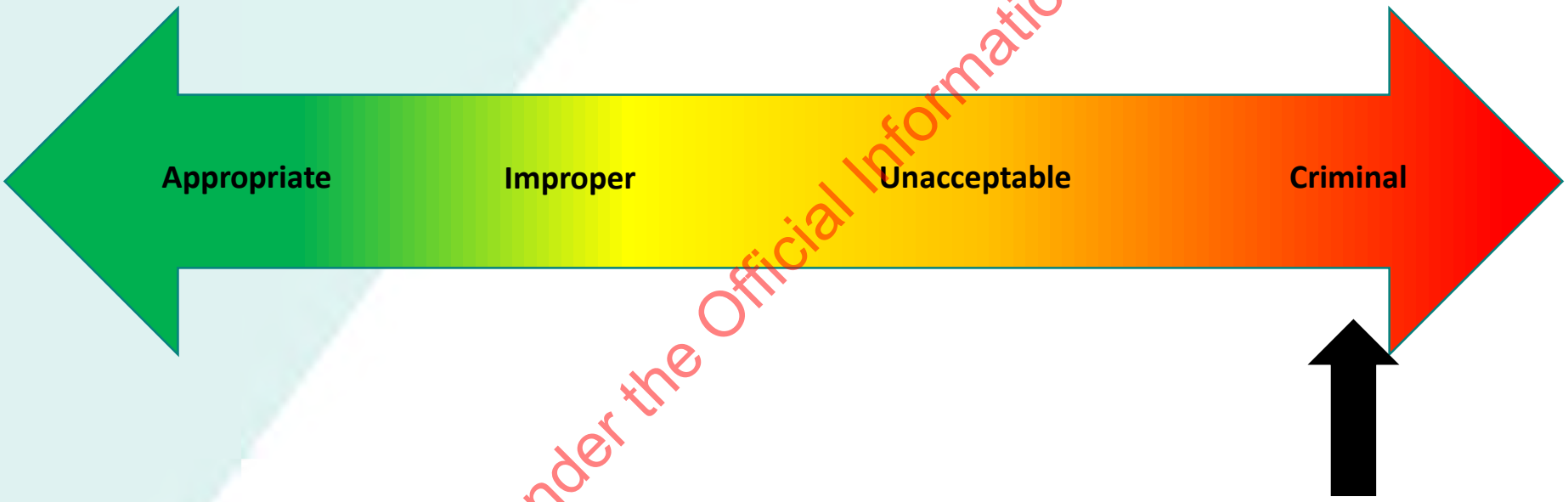
Where does the scenario fit?



Where does the scenario fit?



Where does the scenario fit?

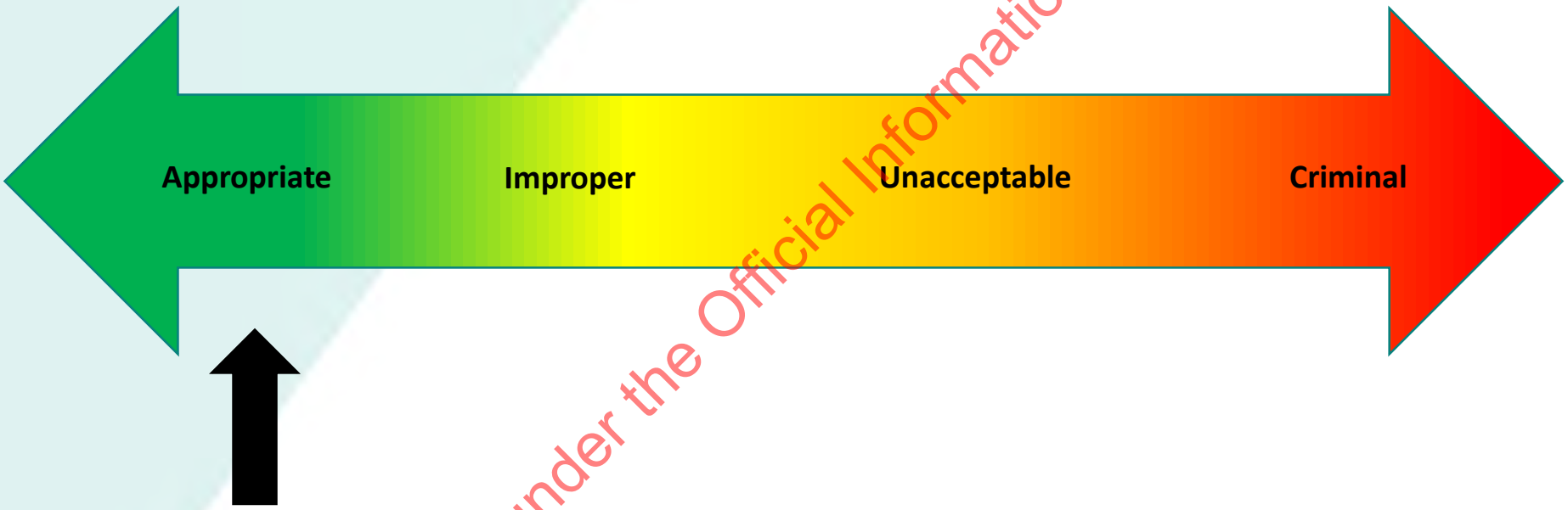


Scenario 2

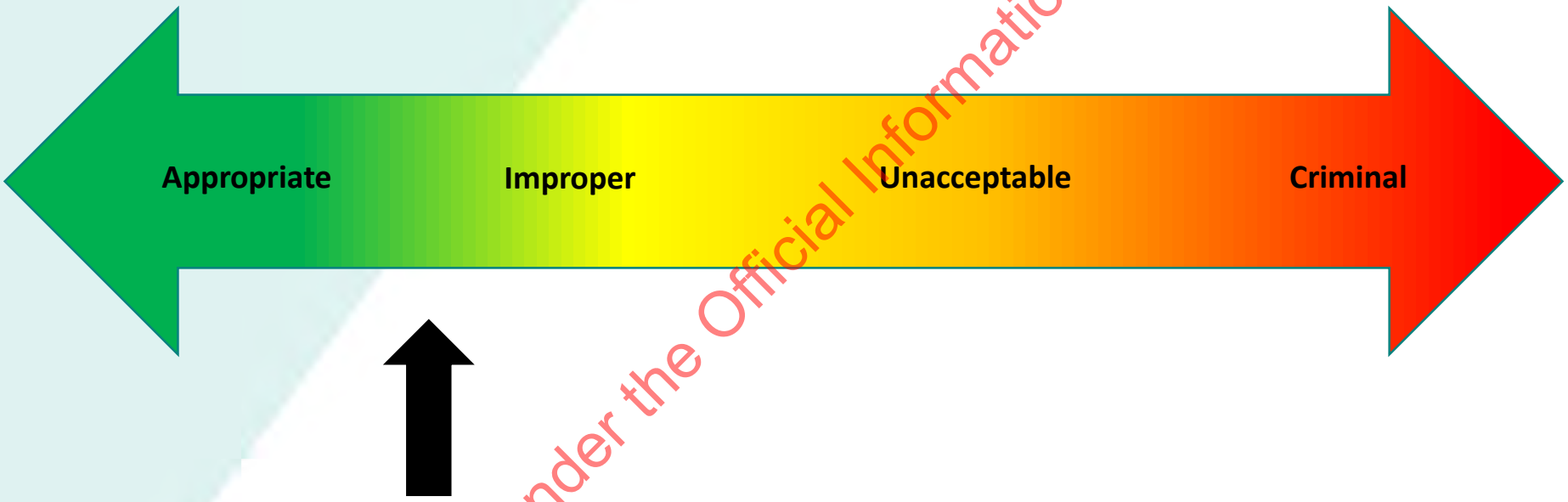
Danielo uses his Facebook account at home to keep up with friends overseas and to share photos. He has just received a message from a friend who has moved back to New Zealand. His friend asks what work he is doing and how he is finding it.

Danielo is feeling pretty stressed at work, and he doesn't like the direction some of the policy is he working on is taking. He takes this opportunity to vent his frustration directly on the wall of his Facebook page.

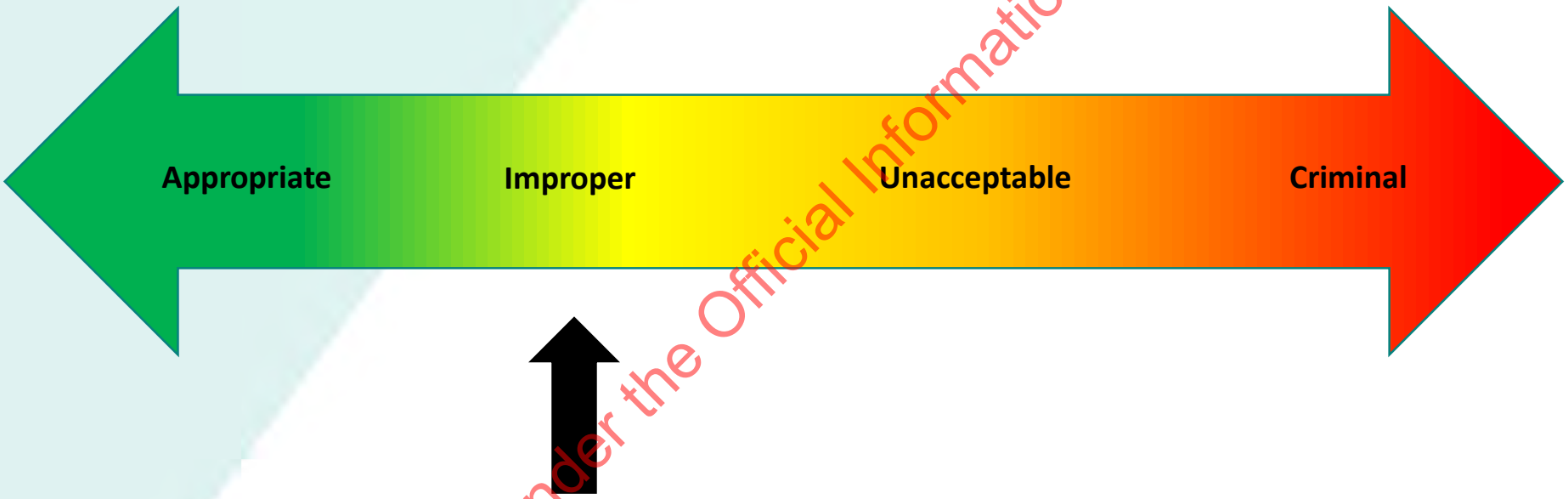
Where does the scenario fit?



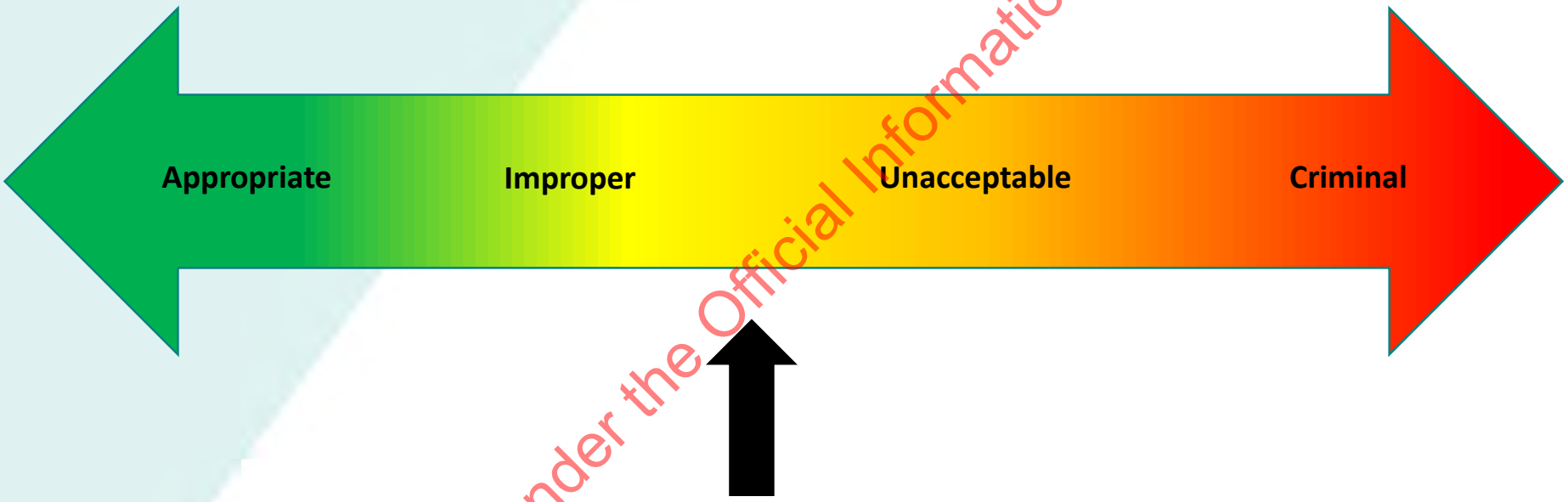
Where does the scenario fit?



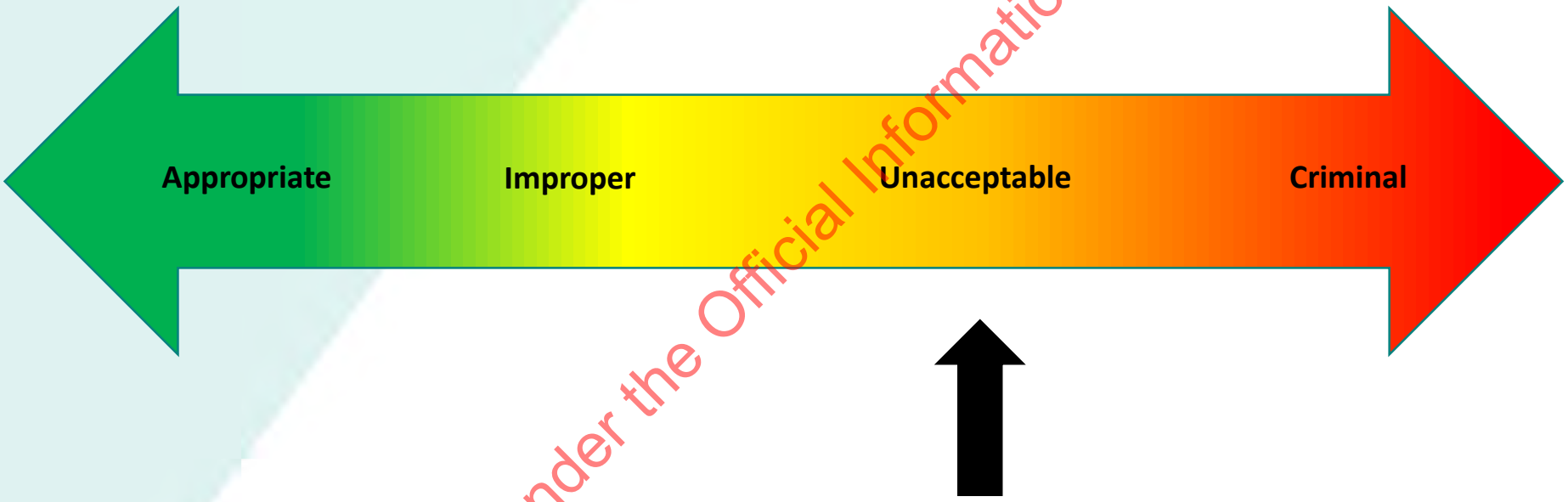
Where does the scenario fit?



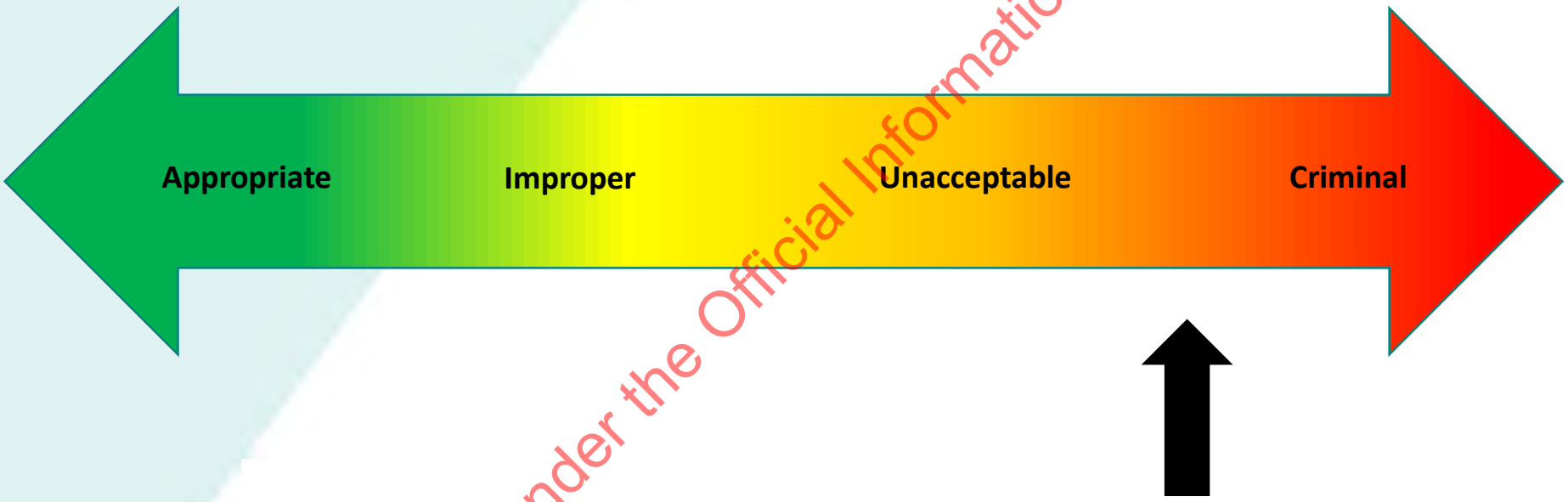
Where does the scenario fit?



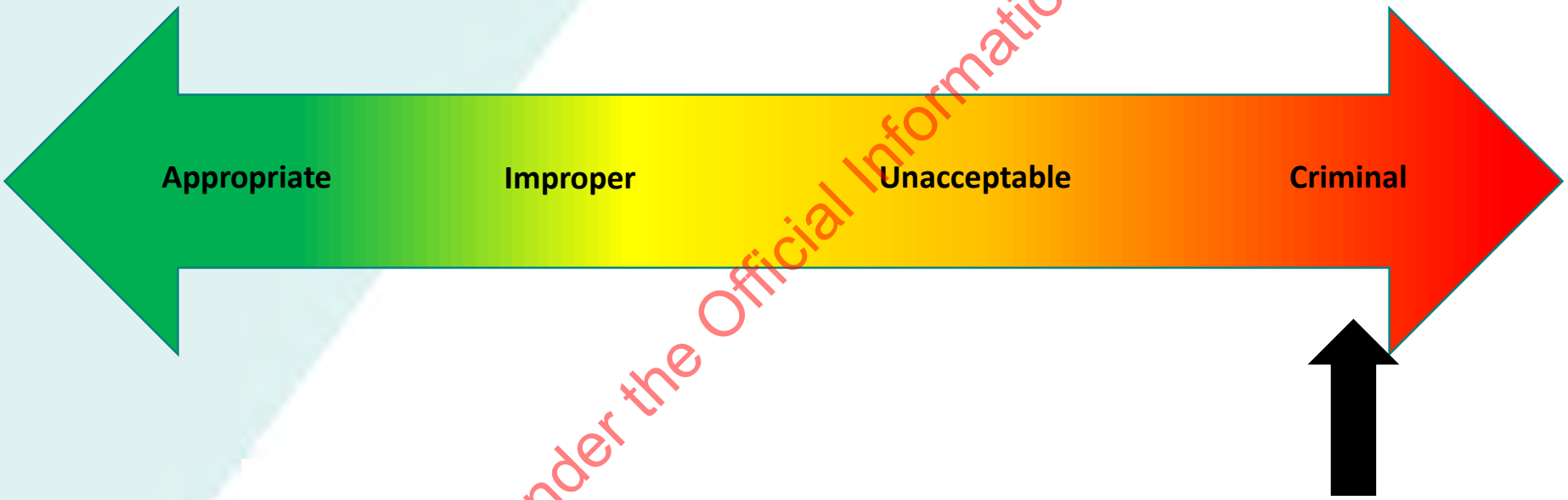
Where does the scenario fit?



Where does the scenario fit?



Where does the scenario fit?



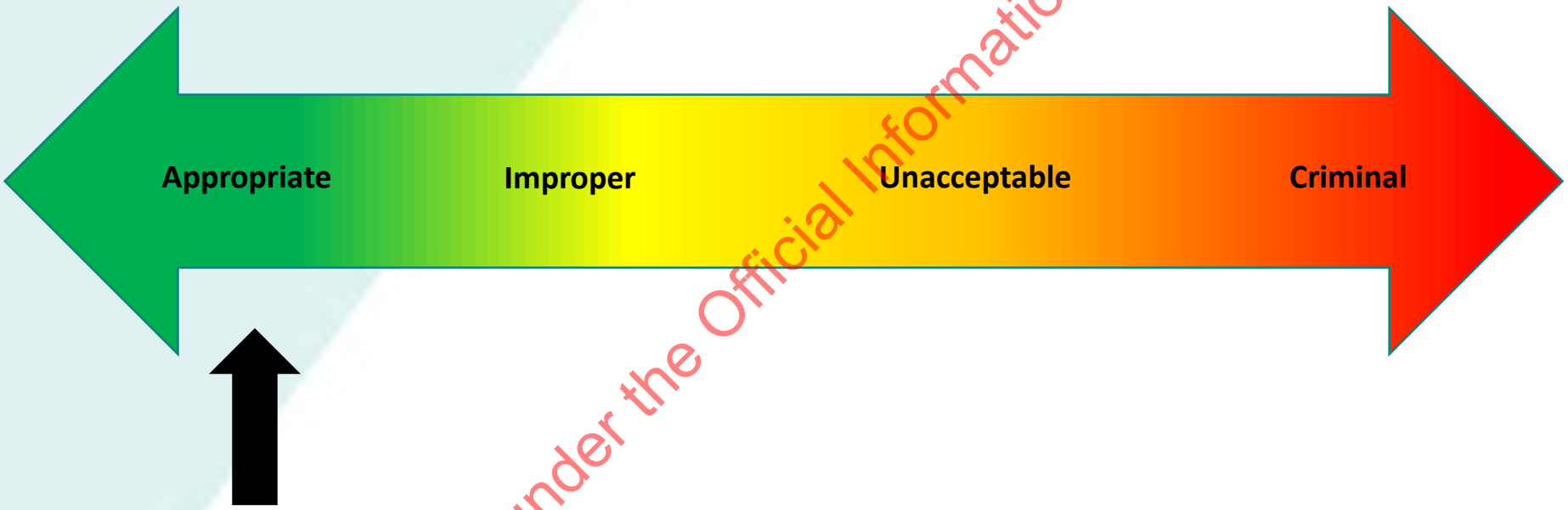
Scenario 3

Miley is finding the constant flow of jokes emailed around her team a bit annoying, and some of them are inappropriate, which is making her feel uncomfortable.

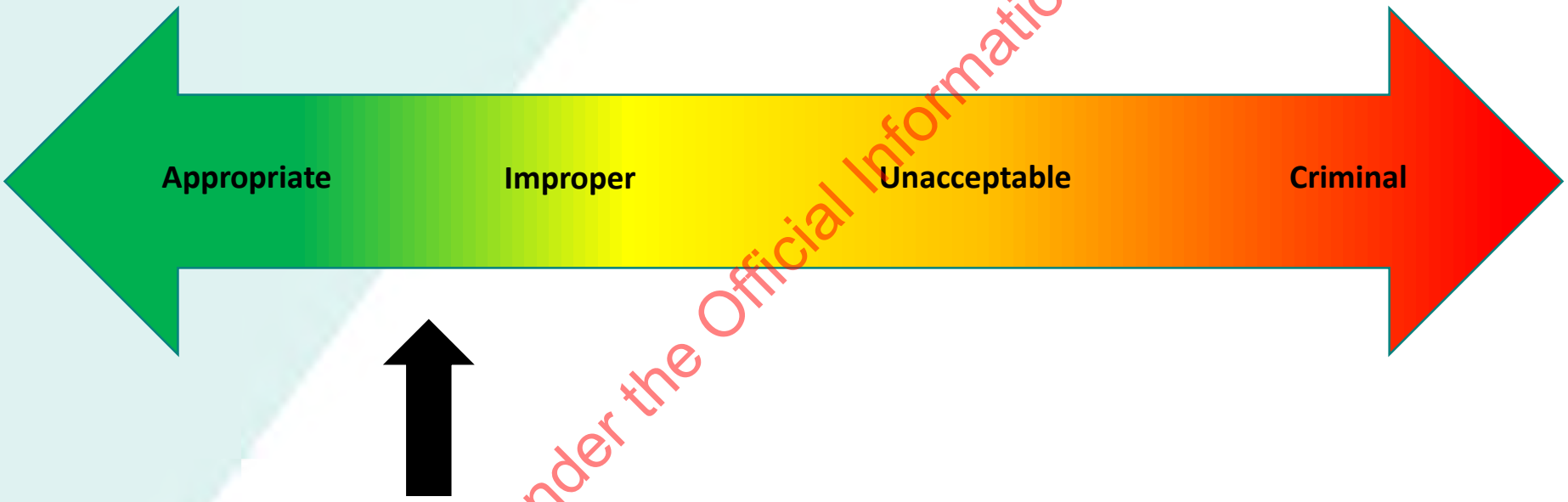
She casually mentions to her workmates that she finds the constant flow of emails distracting and she feels uncomfortable about receiving ‘dirty’ jokes.

When Miley returns to her desk she finds a further joke email.

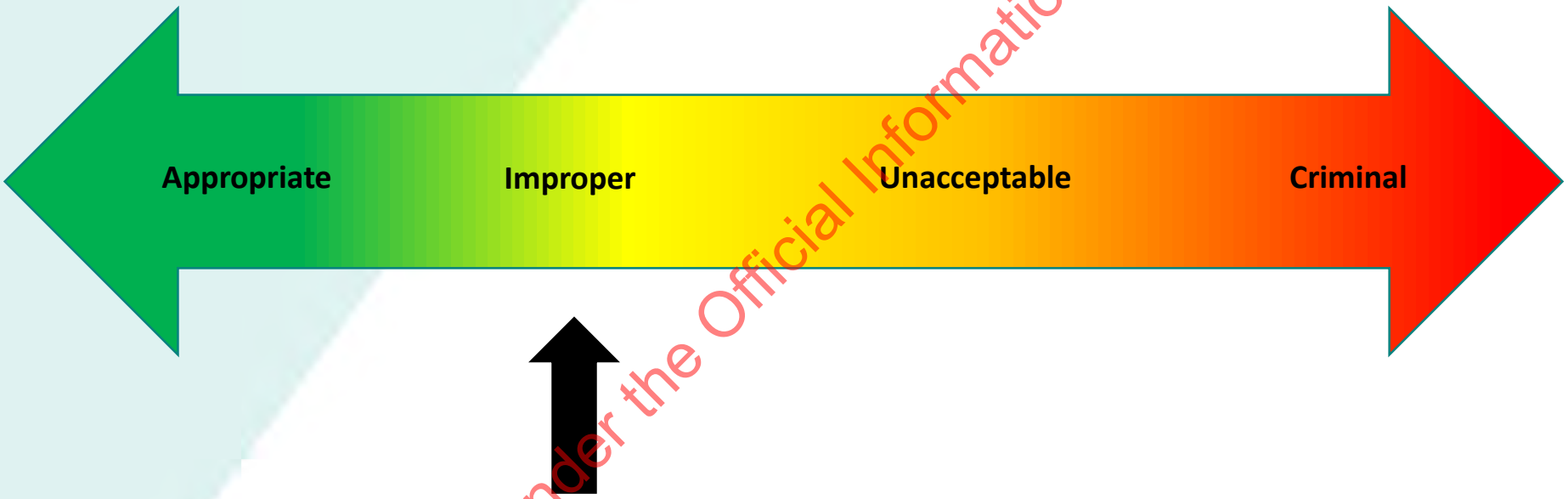
Where does the scenario fit?



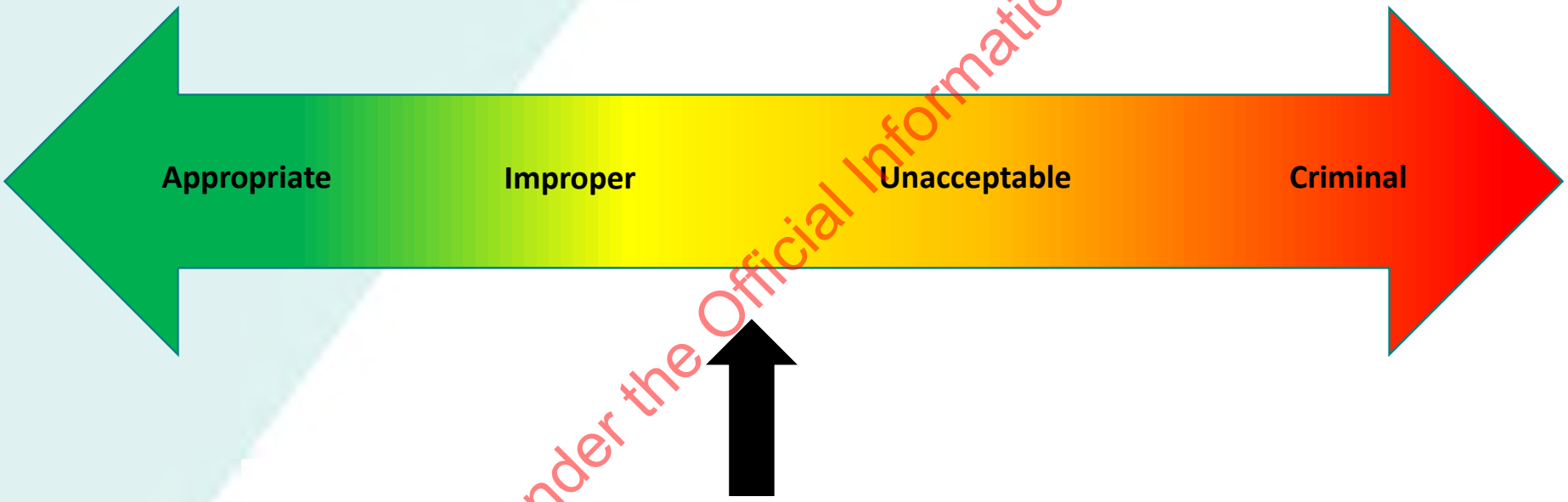
Where does the scenario fit?



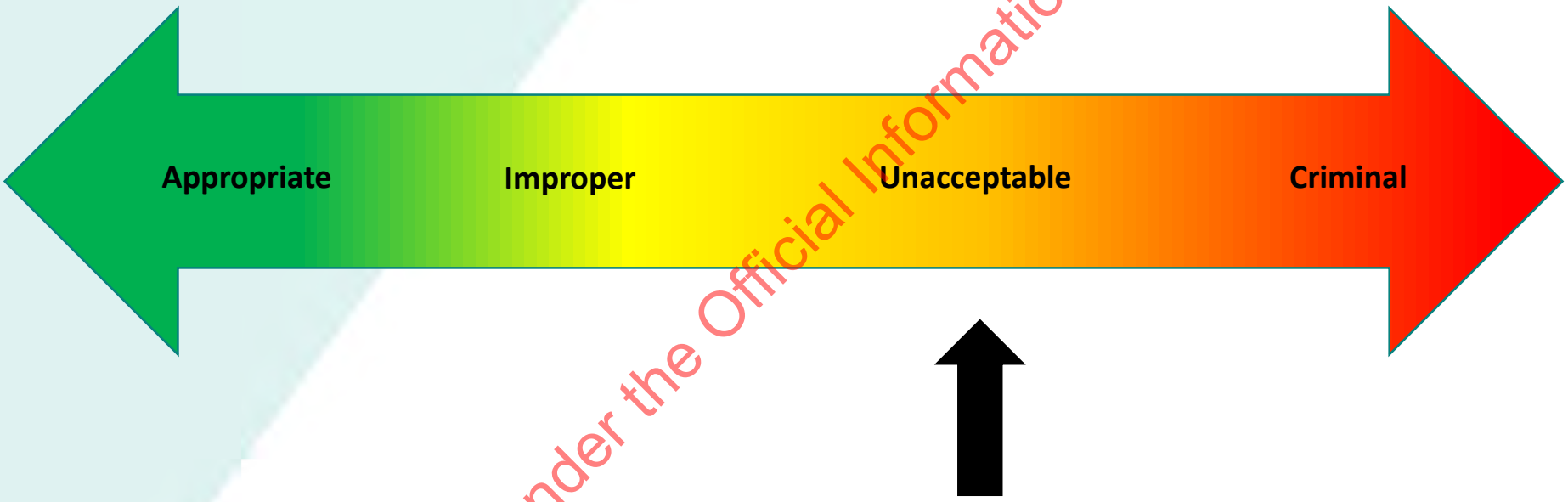
Where does the scenario fit?



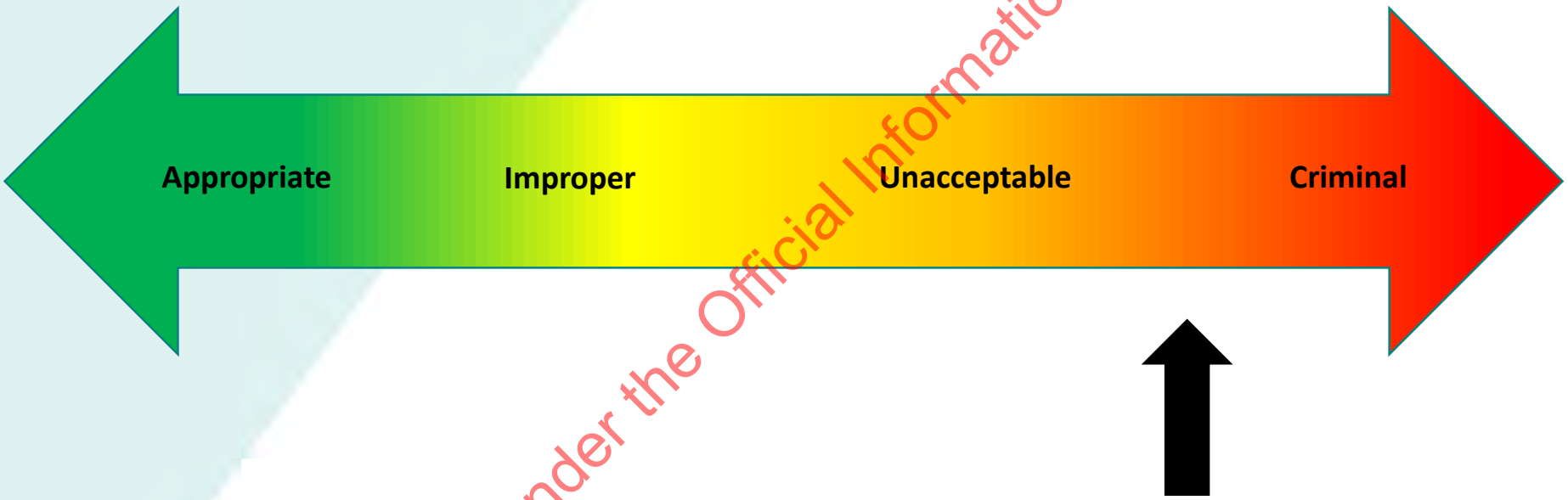
Where does the scenario fit?



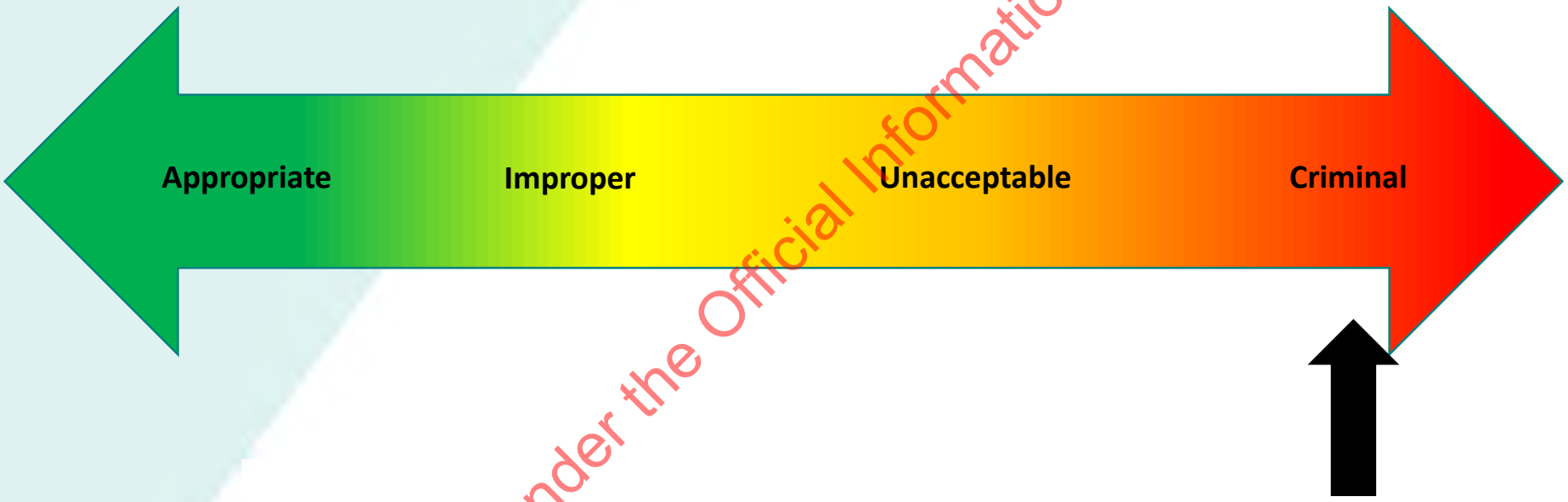
Where does the scenario fit?



Where does the scenario fit?



Where does the scenario fit?



Real examples of integrity matters at Customs

- Escorting family or friends through Customs processes at the airport
- Falsifying a timesheet
- Sexting on a work phone
- Making inappropriate jokes at a meeting
- Reading sensitive documents left by the printer
- Having a glass of wine or a beer on a lunchbreak
- Using illegal drugs
- Using the sickbay to sleep off a hangover
- Having an affair with a colleague

How to speak up if you have concerns

It's safe to speak up

Tell someone:

1. Talk to your manager or any senior leader
2. Talk to a HR Advisor
3. Use the internal reporting form: Integrity Matters
4. Email Integrity@Customs.govt.nz
5. Report to our anonymous 24/7 Integrity Line (external service)

0800 835 269

Security at Customs

Getting the basics right

TE WHAKAMATA
CUSTOMS OFFICER ONBOARDING PROGRAMME

So what IS Security? (And what it Isn't!)

Security is the condition achieved when our information is protected from disclosure, our people are protected from undue influence or subversion and our places and assets are physically secure and always available.

Security is an enabler – good security policy & practice allows us to do our work without interference from those who may have an adverse interest in our activities..

It's NOT about stopping things from being done or beating people over the head with a security manual!!

The effectiveness of ALL security policies, processes, physical & information security compliance regimes rely almost solely on people..

Security in General

Reporting of security incidents

- Immediately report any suspicious activity to your manager and the Customs Security team.
- Note as much information as you can about the incident
- Who, When, Where, and What.

➢ ***If you SEE something; SAY something!!***

➢ https://www.youtube.com/watch?v=IvTJ3cRzVbc

Information Security

Lawful exchange of information

- Understand the legal authority (MoU, Legislation etc) that allows for the information exchange.

Unauthorised access / disclosure

- Insecure information, overheard discussions / phone calls.

Loss or misappropriation of data

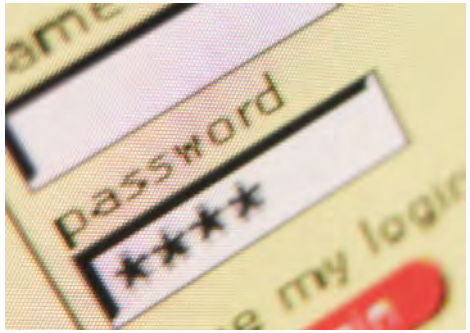
- Information used outside of legal authority to do so.
- Information removed from secure area (via CD, USB, email, hardcopy, mobile phone photos, etc) .

IT & Cyber Security

- Cyber Security identified as one of the world's **biggest** threats
- GCSB identifies Customs as a 'high value' Cyber Security target
- We must **all** protect the system from external and internal threats

Basic Security Measures

- Do not share access to your computer with non-Customs personnel
- Do not share your login ID or password with anyone
- Log-off or lock screen when you leave your computer
- Passwords must be changed every 90 days
- Do not write down your password.



TE WHAKAMATA
CUSTOMS OFFICER ONBOARDING PROGRAMME

Social Media

You're more interesting than you think.

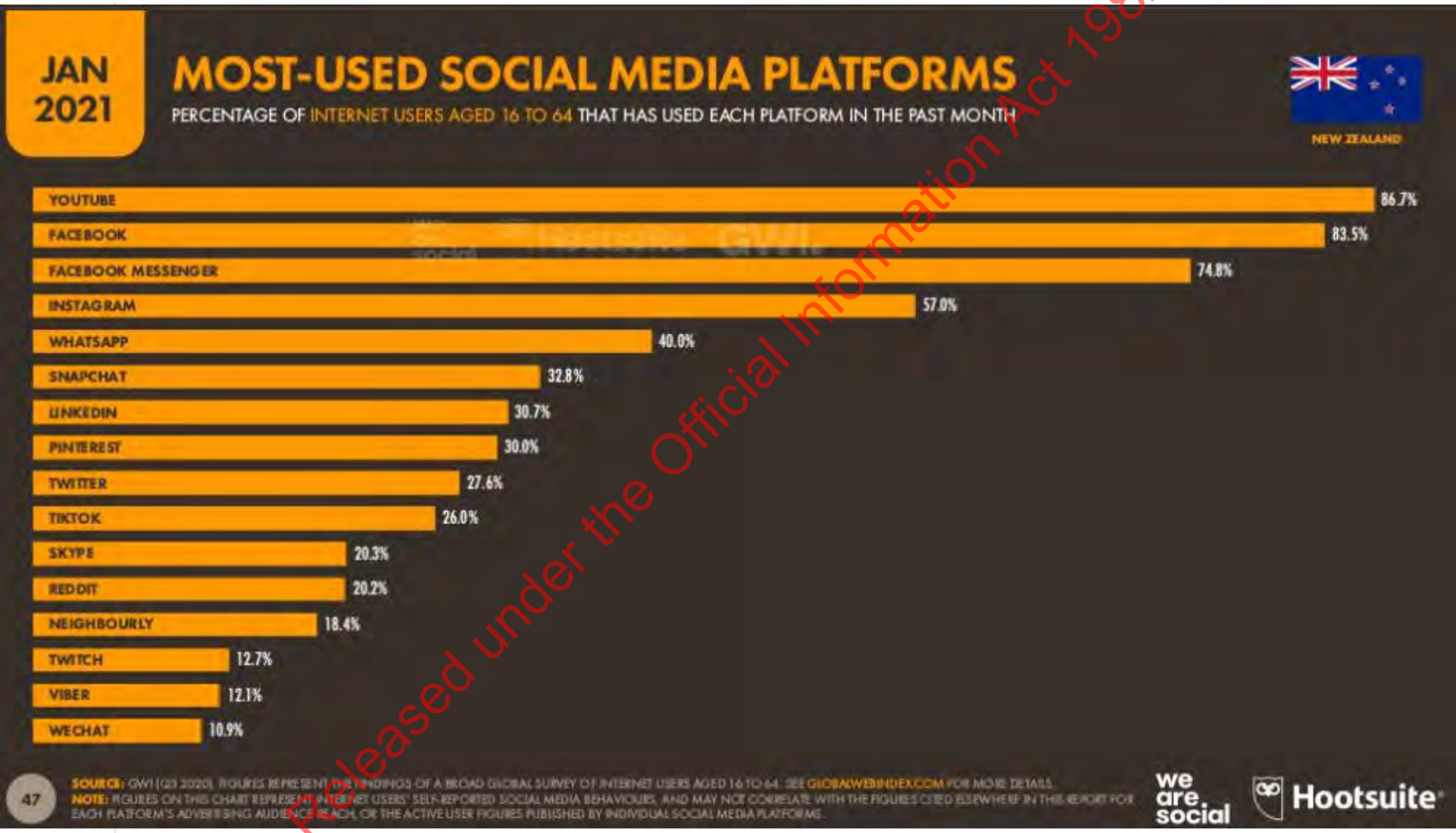
Where you work can make you – and the information about you online – very interesting. Think before you share personal and work-related details. In the wrong hands they could make you, your family or our organisation vulnerable.

Social media landscape 2021

@ItSabrina
@MathieuFlex
@FredCavazza
@CavazzaRomeo

SYSK

And for New Zealand...



Social Media

SLIDE TITLE

- DO NOT disclose any Customs or government material that isn't publicly available.
- DO NOT identify yourself as a Customs officer online.
- DO NOT identify other Customs Officers online.

Social Media

SLIDE TITLE

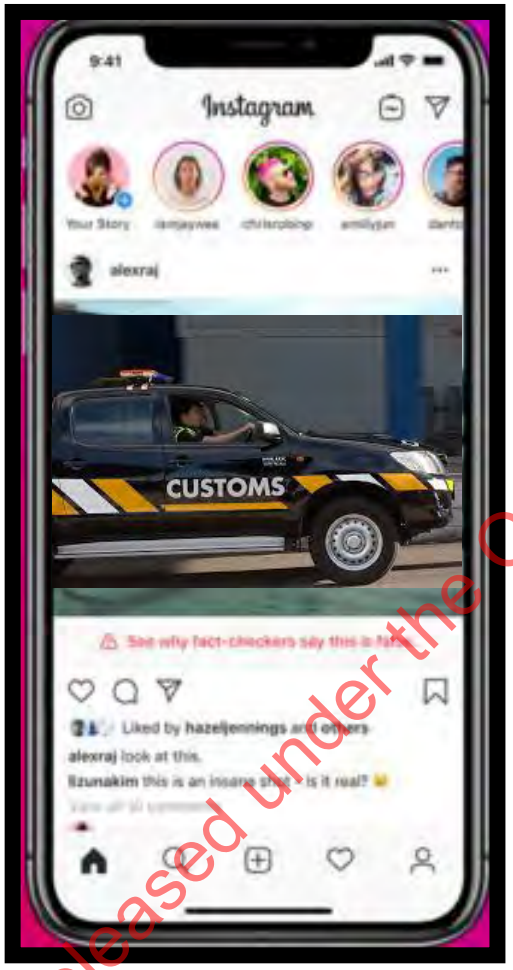
- DO NOT use work computers to make comment on social media. This could potentially be a breach of the Customs Code of Conduct.
- Don't disclose any Customs or government material that isn't publicly available

If in doubt, you should always treat any social media forum as a public forum

Social Engineering

What is it?

- Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques
- Social engineering is often performed by the attacker pretending to be someone they are not.
- It is not just restricted to online activity.



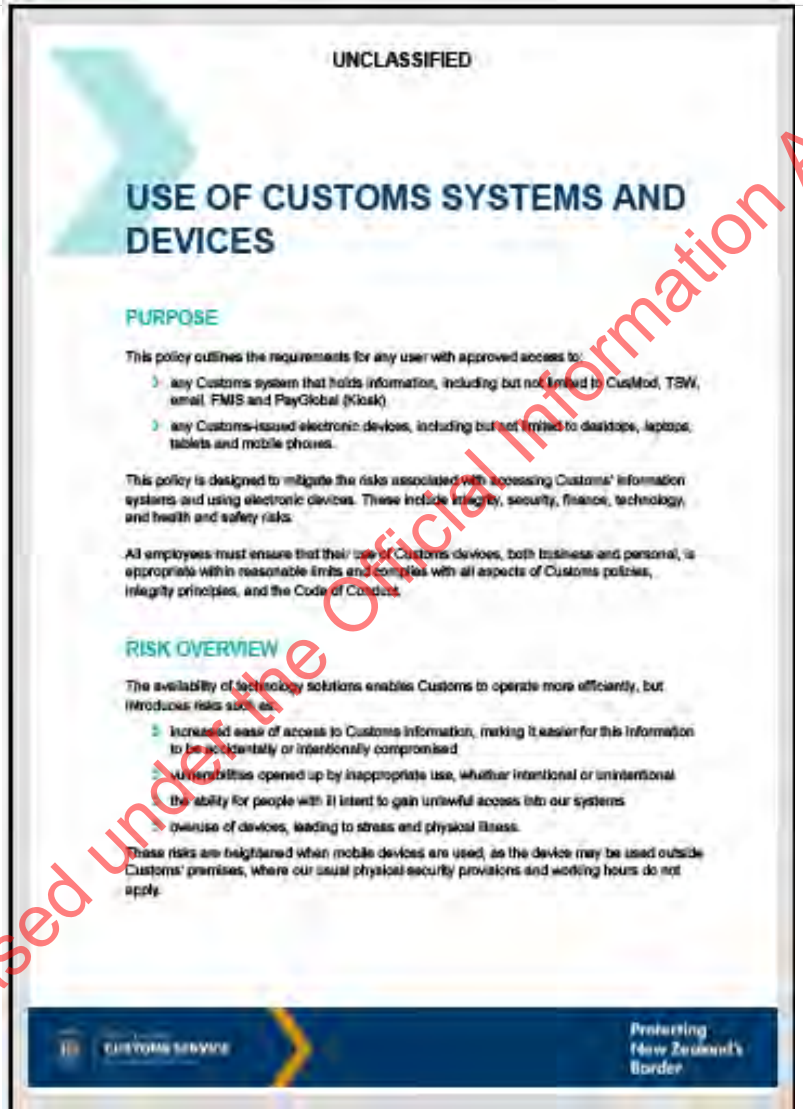
Staying Safe On-line

#livingthedream
#outandaboutatwork
#lovemyjob
#customslove

Make it clear to others when your contribution is as a private individual, not a Customs representative

Use of Customs Systems and Devices

SLIDE TITLE



UNCLASSIFIED

USE OF CUSTOMS SYSTEMS AND DEVICES

PURPOSE

This policy outlines the requirements for any user with approved access to:

- any Customs system that holds information, including but not limited to CusMod, TBW, email, FMIS and PayGlobal (Kiosk)
- any Customs-issued electronic devices, including but not limited to desktops, laptops, tablets and mobile phones.

This policy is designed to mitigate the risks associated with accessing Customs' information systems and using electronic devices. These include integrity, security, finance, technology and health and safety risks.

All employees must ensure that their use of Customs devices, both business and personal, is appropriate within reasonable limits and complies with all aspects of Customs policies, integrity principles, and the Code of Conduct.

RISK OVERVIEW

The availability of technology solutions enables Customs to operate more efficiently, but introduces risks such as:

- increased ease of access to Customs information, making it easier for this information to be accidentally or intentionally compromised
- vulnerabilities opened up by inappropriate use, whether intentional or unintentional
- the ability for people with ill intent to gain unlawful access into our systems
- overuse of devices, leading to stress and physical illness.

These risks are heightened when mobile devices are used, as the device may be used outside Customs' premises, where our usual physical security provisions and working hours do not apply.

CUSTOMS SERVICE

Protecting New Zealand's Border

Computer Security (E-mail)

E-Mail Restrictions

- Do not use Customs e-mail for private business activities, amusement or entertainment.
- Do not send e-mail containing racist, sexist, threatening or other objectionable language.

E-Mail Safety

- Do **not** open unknown or unexpected e-mail attachments! Ever!
- Do not subscribe to personal mailing lists e.g. TreatMe, Facebook, TradeMe
- Think before you give out your work email address, (what will they do with your information)

Removable Media Security

- Do not use non-Customs provided CDs, DVDs and especially USB sticks in Customs PC's
- Do not trust Media given to you, or found lying around
- Never connect a personal electronic device (Phones, Media Players etc) to any Customs IT device.
- Familiarise yourself with Customs Policies.

TE WHAKAMATA
CUSTOMS OFFICER ONBOARDING PROGRAMME

Security

How we stay secure

Customs Information is Valuable!!

What information would we have that is of interest?

- Sensitive Financial Data
- Operations information
- Intelligence
- How we target
- Classified information
- Personal information on customers
- Personal Staff information
- Trade and Tariff information
- Investigative & Surveillance
- SOP/OpsPro

Who would be interested in knowing?

- Local Criminals/Organised Crime Groups – International and Domestic
- Terrorists
- Hackers
- Issue Motivated Groups
- Foreign Intelligence Services
- Disaffected employees
- Competitors
- Foreign States

Protecting Documents

GUIDELINES FOR PROTECTION OF OFFICIAL INFORMATION

SELECTING AN APPROPRAITE SECURITY CLASSIFICATION

curity Classifications

nise could affect the security or defence of
e international relations of the
nent of New Zealand

Policy and Privacy Classifications

information, for which compromise does not threaten the security of the nation, but rather the security or interests of individuals, groups, commercial entities, government business and the community

SENSITIVE

on would be likely to damage the interests of New Zealand or endanger the safety of its citizens

erson.
my of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies

rol of overseas exchange transactions
r credit

djustment of prices of goods and services, rents and other costs, and rates of wages, salaries and other incomes
the Government of New Zealand
s trade agreements.
wn or a department organisation holding the information to carry on without prejudice or disadvantage, negotiations (including
gotiations).

IN-CONFIDENCE

on would be likely to prejudice the maintenance of law and order, impede the effective conduct government in New Zealand or affect adversely the privacy of its citizens.

f law, including the prevention,
f offences, and the right to a fair trial.
of natural persons, including that of

reasonably to prejudice the commercial
upplied or is the subject of the

g the health or safety of members of the

nomic interests of New Zealand.
vent or mitigate material loss to members

viege.
wn or any Department or organisation
ry out, without prejudice or
ctivities.
of official information for improper gain

- Disclose information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied; or be likely otherwise to damage the public interest.
- Breach the constitutional conventions for the time being which protect: the confidentiality of communications by or with the Sovereign or Her representative; collective and individual ministerial responsibility; the political neutrality of officials; and the confidentiality of advice tendered by ministers of the Crown and officials.
- Impede the effective conduct of public affairs through: the free and frank expression of opinion by or between or to Ministers of the Crown or officers and employees of any department or organisation in the course of their duty; the protection of such Ministers, officers and employees from improper pressure or harassment.

TOP SECRET

e of information would damage national interests in an exceptionally grave manner

stability of NZ or friendly countries
oss of life
amage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of extremely valuable
tions
age to relations with other governments
age to significant national infrastructure

SECRET

romise of information would damage national interests in a serious manner

ith friendly governments
e operational effectiveness or security of New Zealand or friendly or the effectiveness of valuable security or intelligence

l stability of New Zealand or friendly countries
srupt significant, national infrastructure

CONFIDENTIAL

omise of information would damage national interests in a significant manner

relations (i.e. cause formal protest or other sanctions)
onal effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or

HANDLING and/or TRANSMITTING POLICY AND PRIVACY INFORMATION

RESTRICTED and SENSITIVE

Principles and Clearance Levels

- Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely.
- Only Staff authorised by the department to access RESTRICTED or SENSITIVE levels are authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.

Electronic Transmission

- All RESTRICTED or SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by GCSB.

Electronic Storage

- Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms:
  - user challenge and authentication (username/password or digital ID/Certificate)
  - logging use at level of individual
  - firewalls and intrusion-detection systems and procedures;
  - server authentication
  - OS-specific/application-specific security measures.

Electronic Disposal

- Electronic files should be disposed of in a way that makes reconstruction highly unlikely.

Manual Transmission

- **Within a single physical location.** As determined by the Chief Executive or Head of the organisation.
- **Transfer between establishments within or outside New Zealand.**
  - May be carried by ordinary postal service or commercial courier firms, provided the envelope/package is closed and the word RESTRICTED or SENSITIVE is not visible.
  - The outer envelope should be addressed to an individual by name and title. RESTRICTED/SENSITIVE mail for/from Overseas posts should be carried by diplomatic airfreight via MFAT.
  - The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.

Manual Storage

- In an office environment, RESTRICTED and SENSITIVE material should be held in a lockable storage area or cabinet.
- In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.

Manual Disposal

- RESTRICTED and SENSITIVE documents are to be disposed of or destroyed in a way that makes reconstruction highly unlikely.

IN-CONFIDEN

Principle and Clearan

- Information for official use, with consi
  principle

Electronic Transmi

- An appropriate statement should acc
  CONFIDENCE information transmit
- It should outline legal responsibilities
  instructions if the incorrect party recei
- IN CONFIDENCE data can be transm
  public networks but the level of inform
  assessed before using clear text.
- Username/Password access control a
  advisable (with the aim of maintaining
  public agencies).
- All IN CONFIDENCE information (incl
  identify the originating government ag

Electronic Stora

- Electronic files (including databases)
  against illicit internal use or intrusion b
  two or more of the following mechanis
  - user challenge and authentication (u
    digital ID/Certificate)
  - logging use at level of individual
  - firewalls and intrusion-detection syst
  - server authentication
  - OS-specific/application-specific secu

Electronic Dispo

- Electronic files should be disposed of
  reconstruction highly unlikely.

Manual Transmiss

- May be carried by ordinary postal ser
  firm as well as mail delivery staff in a
- The envelope must clearly show a ret
  delivery is unsuccessful. In some cas
  concerns, identifying the originating d
  inappropriate and a return PO Box alo

Manual Storag

- IN CONFIDENCE information can be
  building security and door-swipe card
  keep the public out of administrative a
  departments.

Manual Disposa

- Disposed of by departmental arrange

ENDORSEMENTS (may be used with any security classification)

APPOINTMENTS • BUDGET • CABINET • COMMERCIAL • EVALUATIVE • HONOURS • MEDICAL •

HANDLING and/or TRANSMITTING PROTECTIVELY MARKED NATIONAL SECURITY INFORMATION

CONFIDENTIAL

Principles and Clearance Levels

CONFIDENTIAL must be held, processed, transmitted and
security commensurate with the significant damage to national
would incur.
department for CONFIDENTIAL access or above is authorised
. This includes all staff involved with transmission, storage, and

Electronic Transmission

mation transmitted across any networks within New Zealand or
ted using a system approved and accredited by GCSB.

Electronic Storage

databases) must be protected against illicit internal use or
ies through the judicious selection of two or more of the following

entication (username/password or digital ID/Certificate)
ndividual
detection systems and procedures; server authentication
-specific security measures

Electronic Disposal

NFIDENTIAL information must be declassified by degaussing,
iaw GCSB guidelines contained in chapter 12.6 of the *NZISM*.

Manual Transmission

l location. Single opaque envelope that indicates the
t at the discretion of the originator, and either:
partment's own transit system; or
ding or part of a building that has been declared a specially
se
ed and sealed with approved seals in accordance with PSR -
for Protectively Marked Information and Equipment and carried
ly security vetted messengers.
olishments within New Zealand. CONFIDENTIAL material
ped and sealed with approved seals in accordance with PSR -
for Protectively Marked Information and Equipment and:
d messenger or safe-hand courier with "By Hand" stamped on

essenger or safe-hand courier service exists CONFIDENTIAL
signature required commercial courier or registered post.
ed.
olishments outside New Zealand. Confidential material must
"By Hand" stamped on the outer envelope and sealed with
lance with PSR - para 6.1 *Handling Requirements for*
rmation and Equipment with a receipt form included inside the

afe-hand bag service operated by MFAT to or between posts; or
urier service exists material may be sent by registered post within
the United States of America between New Zealand posts
ountries; or
ances CONFIDENTIAL material may be transmitted by registered
and diplomatic posts or other New Zealand agencies situated in
nada, Australia and the United States of America, or by
g between MFAT and New Zealand official missions in Niue and
ice contact NZSIS.
e handled as stated in the Physical Security Management

Manual Storage

ed security container when not in use. See PSR - Table 5 of para4.12

SECRET

Principles and Clearance Levels

- Information classified as SECRET must be held, processed, transmitted and destroyed with levels of security commensurate with the serious damage to national security that compromise would incur.
- Only Staff cleared by the department for SECRET access or above is authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.

Electronic Transmission

- All SECRET information transmitted across any networks within New Zealand or overseas must be encrypted using a system approved and accredited by GCSB.

Electronic Storage

- Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through the judicious selection of two or more of the following mechanisms:
  - user challenge and authentication (username/password or digital ID/Certificate
  - logging use at level of individual
  - firewalls and intrusion-detection systems and procedures; server authentication
  - OS-specific/application-specific security measures

Electronic Disposal

- Media that has held SECRET information must be declassified by degaussing, overwriting or destroying iaw GCSB guidelines contained in chapter 12.6 of the *NZISM*.

Manual Transmission

- **Within a single physical location**. Material should be double enveloped and sealed in accordance with PSR - *Handling Requirements for Protectively Marked Information and Equipment* and:
  - despatched through a department's own transit system with hand-to-hand receipts at each stage of the journey; or
  - distributed within a building or part of a building that has been declared a specially protected area; otherwise
  - carried by authorised messengers.
- **Transfer between establishments within New Zealand.** SECRET material must be double enveloped and sealed with approved seals in accordance with PSR - *Handling Requirements for Protectively Marked Information and Equipment* and carried by authorised, sufficiently security vetted messengers or safe-hand courier.
- **Transfer between establishments outside New Zealand.** SECRET material must be double enveloped and sealed with approved seals in accordance with PSR - *Handling Requirements for Protectively Marked Information and Equipment* with a receipt form included inside the inner envelope and carried by Diplomatic safe-hand bag service operated by MFAT.
- **COMSEC material.** To be handled as stated in the Physical Security Management protocol of PSR

Manual Storage

- Must be locked in an approved security container when not in use. See PSR - Table 5 of para4.12 of Security zones and risk mitigation in the Physical security management protocols. The minimum acceptable storage arrangements are a combination of the protection afforded by the security container itself, the position or site (Security Zone) and the use of approved security equipment.

Manual Disposal

- If accountable, the destruction should be recorded by marking the record of accountable documents or the file index sheet where these are used. See PSR Section 9 of *Handling Requirements for Protectively Marked Information and Equipment*
- Destroy by burning, pulping, shredding or dry maceration.

FOR FURTHER INFORMATION REFER TO:

TOP SECRET

Principles and Clearance Levels

- Information classified as TOP SECRET must be held, process
destroyed with levels of security commensurate with the exce
national interest that compromise would incur.
- Only staff cleared by the department for TOP SECRET acces
information. This includes all staff involved with transmission,

Electronic Transmission

- All TOP SECRET information transmitted across any network
overseas must be encrypted using a system approved and ac

Electronic Storage

- Electronic files (including databases) must be protected again
intrusion by external parties through the judicious selection of
mechanisms:
  - user challenge and authentication (username/password or d
  - logging use at level of individual
  - firewalls and intrusion-detection systems and procedures; se
  - OS-specific/application-specific security measures

Reproduction

- All TOP SECRET information must be made ACCOUNTABLE
- Once disseminated, ACCOUNTABLE MATERIAL must not be
any form. If additional copies are required, they must be requ
source.

Electronic Disposal

- Media that has held TOP SECRET information cannot be dec
destroyed iaw GCSB guidelines contained in chapter 12.6 of

Manual Transmission

- **Within a single physical location.** Material must be double
approved seals in accordance with PSR - *Handling Requirer*
Marked Information and Equipment and carried by authorised
messengers
  - dispatched through a department's own transit system with
  each stage of the journey; or
  - distributed within a building or part of a building that has bee
  protected area (SCIF); otherwise
  - carried by authorised messengers within an NZSIS approve
- **Transfer between establishments within New Zealand.** TO
be double enveloped and sealed with approved seals in accor
Requirements for Protectively Marked Information and Equipm
authorised, sufficiently security vetted messengers
- **Transfer between establishments outside New Zealand.** T
be double enveloped and sealed with approved seals in accor
Requirements for Protectively Marked Information and Equipm
included inside the inner envelope and carried by the Diploma
operated by MFAT.
- **COMSEC material.** To be handled as stated in the Physical
protocol of PSR

Manual Storage

- Must be locked in an approved security container when not in
para 4.12 of Security Zones and Risk Mitigation in the Physica
protocols
- The minimum acceptable storage arrangements are a combin
afforded by the security container itself, the position or site (S
approved security equipment.

IN CONFIDENCE

NEW ZEALAND CUSTOMS SERVICE

OPS PRO 071

ENTRY OF IMPORTED GOODS PROCEDURE

This document reflects changes to the 2018 Act and changes to the de minimis from 1 December 2019. Other aspects of the document have not been checked for accuracy and to confirm that they are current. This will occur when the document is next due for review.

Amendment to sections on re-import of goods previously exported.

Issued: 12 February 2015
Updated: 1 December 2019
Review due: 1 September 2016

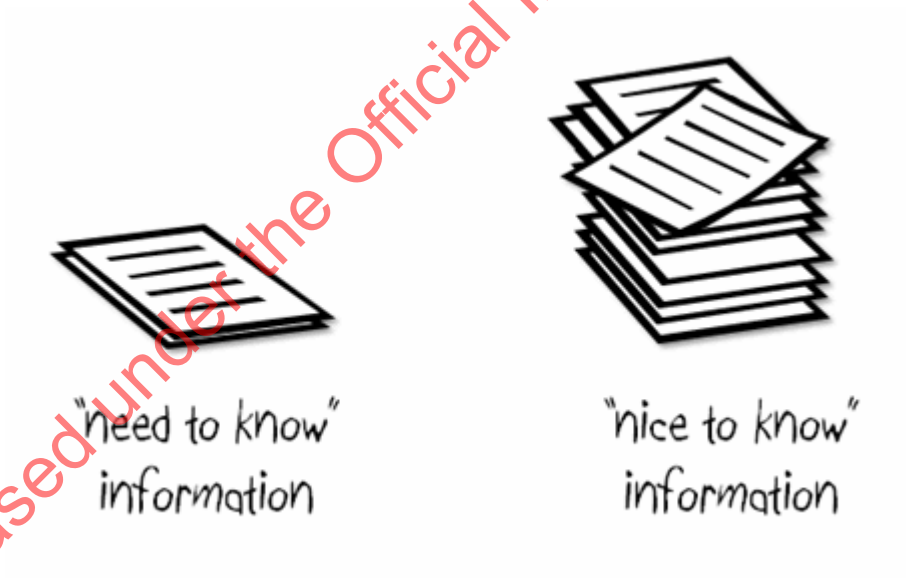
PURPOSE

1. This document contains the procedure for the entry for importation of goods, including both computerised and manual entries, exemptions and re-importation.

CONTENTS

The information in this document is classified as IN CONFIDENCE and is provided for the use of Customs officers only. The information is not to be released or copied without prior consent.

Do you “Need to know”?

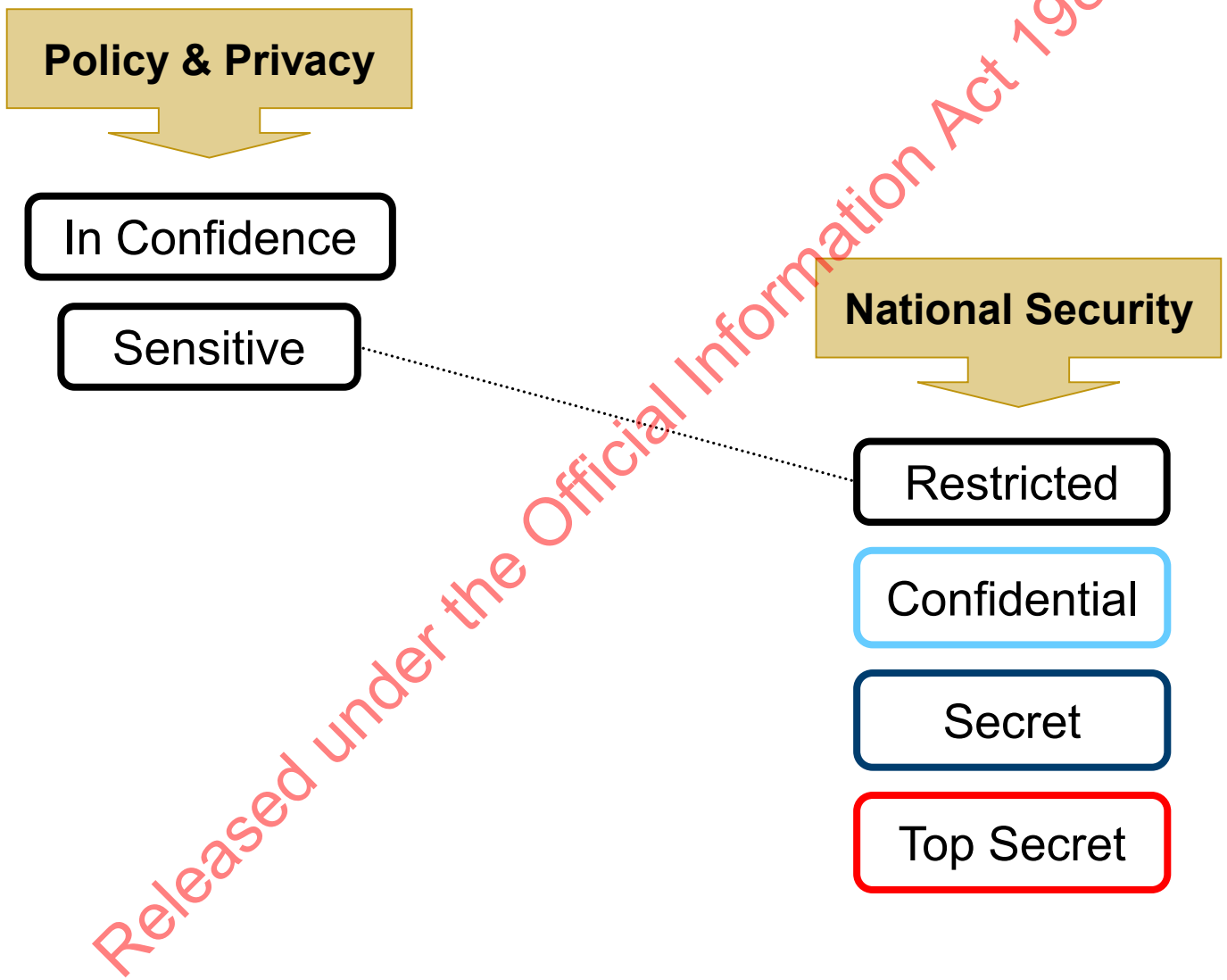


Classification and Information Handling

What is an asset?

- An 'asset' is anything of value to and necessary for an organisation's core business...
- People and their skills
- Information and Information systems
- Operational knowledge
- Equipment
- Money
- Vehicles and property

Types of Classification



Protecting our Assets (Information)

RESTRICTED (National Security)

- Compromise of information would be likely to affect the national interests in an adverse manner.

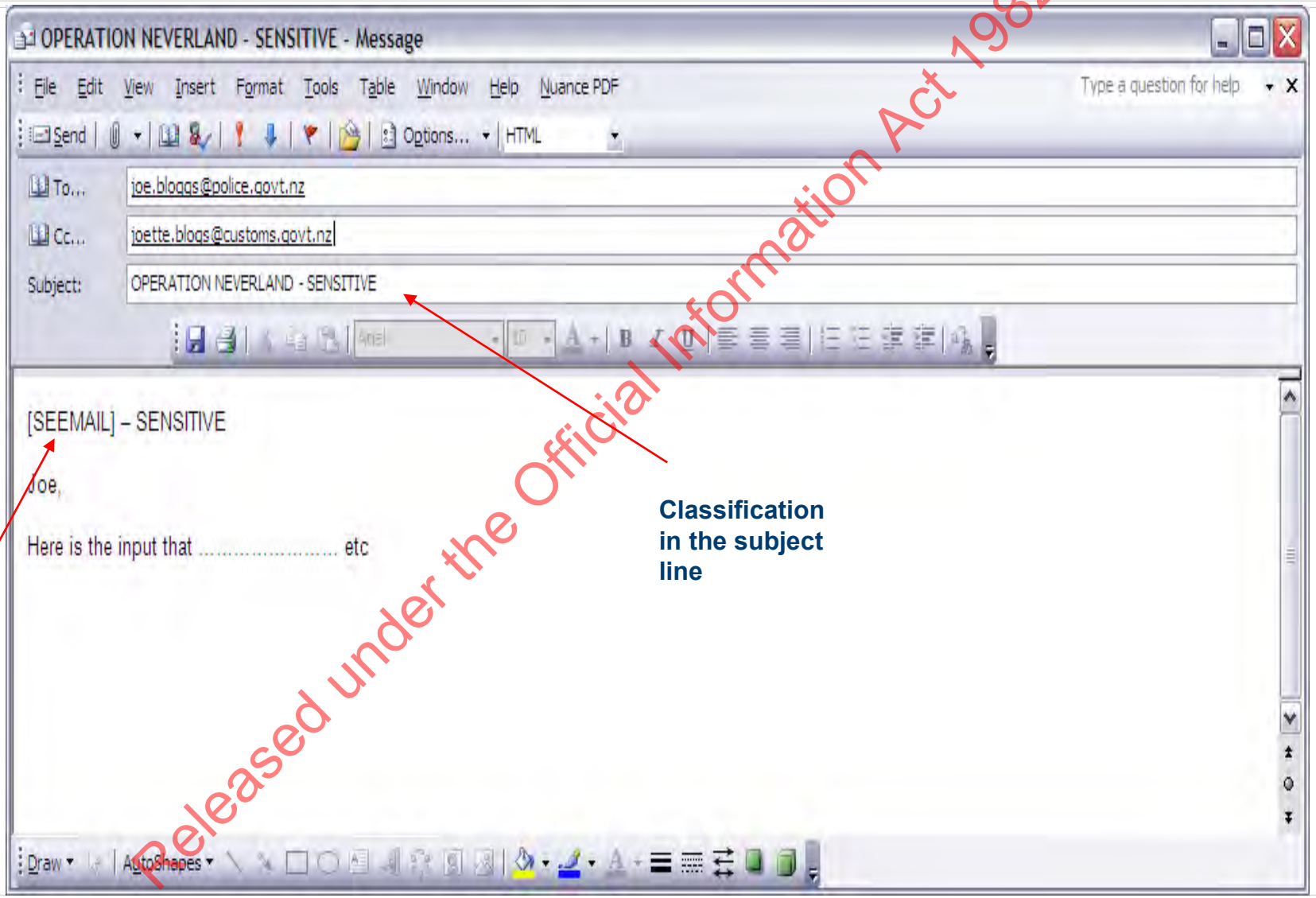
SENSITIVE (Policy & Privacy)

- Compromise of information would be likely to damage the interests of New Zealand or endanger the safety of its citizens.

IN CONFIDENCE (Policy & Privacy)

- Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens.

How to send [SEEMAIL]



Must put this here

Classification in the subject line

Resources

Resources

- **The Longroom**
  - Internet and email policy (SEC POL 04)
  - Guidelines for Protections of Official Information
  - Customs Security Policies
- **Customs Security Officers**
  - s9(2)(g)(ii) – Senior Security Advisor
  - s9(2)(g)(ii) – Cyber Security Advisor
  - s9(2)(g)(ii) – Security Advisor
- **Protective Security Requirements (PSR)** – www.protectivesecurity.govt.nz

Our Expectations:

You will:

- ✓ Comply with all Security Policies & Instructions
- ✓ Report all security incidents
- ✓ Report unusual activities
- ✓ Disclose any conflicts of interest
- ✓ Report any requests for favours or information on how we operate
- ✓ Protect Customs information and methods of operation; and not disclose this should you move on from Customs.

BE SECURITY AWARE

- ALWAYS wear your IDs and challenge those who are not.
- LOCK any computers when you are away from your desk.
- DO NOT continue sensitive discussions outside the briefing/meeting room.
- PUT AWAY Official or Sensitive documents being left out for anyone passing by to see.
- Sensitive materials being destroyed inappropriately, such as not using a shredder.
- Challenge Staff ignoring security policies and measures.
- Non-Disclosure of Official Information
- 'Out of Work' behaviour including Social Media activities
- Approaches from those seeking favours

s6(c) [redacted]

s6(c) [redacted]

s6(c) [redacted]

Questions?