Table 1. Total keyword loss of specificity

ISP	Actionable advice	Other information	Total	Total keyword loss of specificity (%)
1	17	7	24	29,2
2	5	12	17	70,6
Sum	22	19	41	46,3

Table 2. Number of keywords for actionable advice

ISP	Never	Need	Should	Not	Forbidden	Must	Shall
1	1	2	1	4	1	4	4
2	0	0	0	3	0	2	0
Sum	1	2	1	7	1	6	4
% of all AA	4,5%	9,1%	4,5%	31,8%	4,5%	27,3%	18,2%

Table 3. Number of keywords for other information

ISP	Never	Need	Should	Not	Forbidden	Must	Shall
1	0	0	0	2	0	1	4
2	0	0	1	3	0	4	4
Sum	0	0	1	5	0	5	8
% of all OI	0,0%	0,0%	5,3%	26,3%	0,0%	26,3%	42,1%

Table 4. Keyword loss of specificity

ISP	Never (%)	Need (%)	Should (%)	Not (%)	Forbidden (%)	Must (%)	Shall (%)
1	0	0	0	33	0	20	50
2	-	-	100	50	-	67	100
Sum*	0	0	50	42	0	45	67

Note: *Calculated using the sums in Tables 2 and 3

ISP ID	ISP Name	Keyword	Classification	Sentence	Keyword Instance	Position
1	english_test_isp_1	Never	AA	Never share your password with anyone else, either internally or externally.	Never	0-5
1	english_test_isp_1	Need	AA	o You need to verify the sender's identity if you are uncertain, especially when requests seem unusual or urgent.	need	6-10
1	english_test_isp_1	Need	AA	You need to ensure data is securely disposed of when no longer required.	need	4-8
1	english_test_isp_1	Should	AA	o You should use a password manager to handle your passwords securely.	should	6-12
1	english_test_isp_1	Not	AA	Do not click on unknown links or open unexpected attachments.	not	3-6
1	english_test_isp_1	Not	AA	• 3.3 Physical Security: o Do not leave sensitive documents visible on your desk when unattended.	not	32-35
1	english_test_isp_1	Not	AA	o Installation of software that is not approved by the IT department is strictly forbidden.	not	35-38
1	english_test_isp_1	Not	AA	Sensitive information must not be stored in unsecured locations like personal cloud services or unapproved USB drives.	not	27-30
1	english_test_isp_1	Not	OI	Good cybersecurity is not solely the responsibility of the IT department, but everyone's.	not	22-25
1	english_test_isp_1	Not	OI	Non -compliance is not acceptable; breaches of this policy may lead to disciplinary action, up to and including dismissal, and potentially legal consequences.	not	19-22
1	english_test_isp_1	Forbidden	AA	o Installation of software that is not approved by the IT department is strictly forbidden.	forbidden	83-92
1	english_test_isp_1	Must	AA	o Your computer screen must be locked when you leave your workstation, even for short periods, to prevent unauthorised access.	must	23-27
1	english_test_isp_1	Must	AA	o Systems and software must be kept updated according to the IT department's instructions.	must	23-27
1	english_test_isp_1	Must	AA	Sensitive information must not be stored in unsecured locations like personal cloud services or unapproved USB drives.	must	22-26
1	english_test_isp_1	Must	AA	Incident Reporting All suspected or confirmed security incidents (e.g., suspected breaches, lost equipment, virus infections, phishing attempts) must be reported immediately to the IT helpdesk or your line manager, following the current incident management procedure.	must	147-151
1	english_test_isp_1	Must	OI	Every employee must understand and adhere to these guidelines.	must	15-19
1	english_test_isp_1	Shall	AA	o Passwords shall be complex and changed regularly according to IT department recommendations.	shall	12-17
1	english_test_isp_1	Shall	AA	o Sensitive information shall only be sent via approved and encrypted channels.	shall	24-29
1	english_test_isp_1	Shall	AA	o Visitors shall always be signed in and wear a visible visitor badge.	shall	11-16
1	english_test_isp_1	Shall	AA	Any suspected malicious activity on your computer shall be reported immediately.	shall	50-55

1	english_test_isp_1	Shall	OI	This policy shall guide all employees in their daily activities to protect the company's information assets.	shall	13-18
1	english_test_isp_1	Shall	OI	Data Handling (Strategic & Operational Element) All company data shall be handled according to current legislation (e.g., GDPR) and internal classification rules.	shall	67-72
1	english_test_isp_1	Shall	OI	Managers shall ensure their teams are aware of and understand the policy.	shall	9-14
1	english_test_isp_1	Shall	OI	Review and Updates This policy shall be reviewed and, if necessary, updated at least annually, or more frequently if circumstances require (e.g., changes in the threat landscape or regulations).	shall	33-38
2	english_test_isp_2	Should	OI	• Accountability: All actions within systems should be traceable to a responsible individual or process.	should	46-52
2	english_test_isp_2	Not	AA	Operational Guidelines and Responsibilities (Daily Work) To achieve our strategic objectives and uphold these principles, the following is required from every employee in their daily work: • 4.1 User Accounts and Passwords: o Your user account is personal and must not be shared.	not	271-274
2	english_test_isp_2	Not	AA	Keep sensitive materials locked away when not in use.	not	43-46
2	english_test_isp_2	Not	AA	o Do not store or process company information on personal devices or unapproved cloud services without explicit authorisation.	not	5-8
2	english_test_isp_2	Not	OI	Information security is not merely a technical function; it is a strategic imperative for building and maintaining this trust, protecting our brand reputation, and ensuring our long-term competitiveness and success.	not	24-27
2	english_test_isp_2	Not	OI	Flexibility must not compromise our strategic commitment to security.	not	17-20
2	english_test_isp_2	Not	OI	Non- compliance risks not only operati onal disruption but can severely damage the company's strategic assets , such as brand reputation and client trust.	not	22-25
2	english_test_isp_2	Must	AA	Operational Guidelines and Responsibilities (Daily Work) To achieve our strategic objectives and uphold these principles, the following is required from every employee in their daily work: • 4.1 User Accounts and Passwords: o Your user account is personal and must not be shared.	must	266-270

2	english_test_isp_2	Must	AA	Incident Management All suspected or actual information security incidents (e.g., viruses, data breaches, lost equipment, suspected unauthorised access) must be reported immediately to the IT Helpdesk or your line manager, following the established procedure.	must	155-159
2	english_test_isp_2	Must	OI	Fundamental Security Principles (Strategic Basis for Operational Rules) All handling of information and systems within Examplecorp ABC shall be guided by the following principles: • Confidentiality: Information must only be accessible to authorised individuals.	must	216-220
2	english_test_isp_2	Must	OI	• Integrity: Information must be accurate, complete, and protected from unauthorised modification or deletion.	must	26-30
2	english_test_isp_2	Must	OI	• Availability: Information and associated systems must be accessible to authorised users when needed.	must	52-56
2	english_test_isp_2	Must	OI	Flexibility must not compromise our strategic commitment to security.	must	12-16
2	english_test_isp_2	Shall	OI	Fundamental Security Principles (Strategic Basis for Operational Rules) All handling of information and systems within Examplecorp ABC shall be guided by the following principles: • Confidentiality: Information must only be accessible to authorised individuals.	shall	137-142
2	english_test_isp_2	Shall	OI	• Least Privilege: Users shall only be granted the access necessary to perform their job functions.	shall	26-31
2	english_test_isp_2	Shall	OI	• Risk -Based Approach: Security measures shall be based on assessed risks and proportionate to the value and sensitivity of the information.	shall	43-48
2	english_test_isp_2	Shall	OI	Policy Review and Continuous Improvement This policy shall be reviewed at least annually, or as needed, by the designated function (e.g., Information Security Committee or Head of IT) to ensure it remains current, relevant, and effectively supports the organisation's strategic goals while adapting to the evolving threat landscape.	shall	55-60