Table 1. Total keyword loss of specificity

ISP	Actionable advice	Other information	Total	Total keyword loss of specificity (%)
1	14	9	23	39,1
2	6	12	18	66,7
Sum	20	21	41	51,2

Table 2. Number of keywords for actionable advice

ISP	Aldrig	Behöver	Bör	Ej	Förbjuden	Inte	Måste	Ska	Skall
1	1	1	1	1	1	4	1	2	2
2	0	0	0	0	1	4	0	1	0
Sum	1	1	1	1	2	8	1	3	2
% of all AA	5,0%	5,0%	5,0%	5,0%	10,0%	40,0%	5,0%	15,0%	10,0%

Table 3. Number of keywords for other information

ISP	Aldrig	Behöver	Bör	Ej	Förbjuden	Inte	Måste	Ska	Skall
1	0	2	0	0	0	3	1	2	1
2	0	0	0	0	0	3	0	9	0
Sum	0	2	0	0	0	6	1	11	1
% of all OI	0,0%	9,5%	0,0%	0,0%	0,0%	28,6%	4,8%	52,4%	4,8%

Table 4. Keyword loss of specificity

ISP	Aldrig (%)	Behöver (%)	Bör (%)	Ej (%)	Förbjuden (%)	Inte (%)	Måste (%)	Ska (%)	Skall (%)
1	0	67	0	0	0	43	50	50	33
2	-	-	-	-	0	43	-	90	-
Sum*	0	67	0	0	0	43	50	79	33

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

ISP ID	ISP Name	Keyword	Classification	Sentence	Keyword Instance	Position
1	swedish_test_isp_1	Aldrig	AA	Dela aldrig ditt lösenord med någon annan, varken internt eller externt.	aldrig	5-11
1	swedish_test_isp_1	Behöver	AA	o Du behöver vara extra uppmärksam på avsändaradressen vid extern kommunikation för att undvika nätfiske (phishing).	behöver	5-12
1	swedish_test_isp_1	Behöver	OI	Datahantering och Klassificering (Strategiskt och Operativt) All information som hanteras inom Exempelföretaget ABC har ett värde och behöver skyddas utifrån dess känslighet.	behöver	135-142
1	swedish_test_isp_1	Behöver	OI	Du behöver inte tveka att fråga om något är oklart.	behöver	3-10
1	swedish_test_isp_1	Bör	AA	o Du bör aktivera multifaktorautentisering (MFA) där det erbjuds.	bör	5-8
1	swedish_test_isp_1	Ej	AA	Klicka ej på misstänkta länkar och öppna inte oväntade bilagor.	ej	7-9
1	swedish_test_isp_1	Förbjuden	AA	o Installation av icke -godkänd programvara eller anslutning av privat utrustning till företagets nätverk utan tillstånd är strängt förbjuden.	förbjuden	133-142
1	swedish_test_isp_1	Inte	AA	Klicka ej på misstänkta länkar och öppna inte oväntade bilagor.	inte	42-46
1	swedish_test_isp_1	Inte	AA	o Skicka inte känslig eller konfidentiell information via okrypterad e -post.	inte	9-13
1	swedish_test_isp_1	Inte	AA	• 3.3 Fysisk Säkerhet: o Lämna inte känsliga dokument synliga på skrivbordet när du lämnar det obevakat.	inte	33-37
1	swedish_test_isp_1	Inte	AA	Lagring av känslig företagsinformation på privata enheter eller molntjänster är som huvudregel inte tillåten.	inte	96-100
1	swedish_test_isp_1	Inte	OI	Att upprätthålla hög säkerhet är inte en engångsinsats, utan en kontinuerlig process som kräver vaksamhet från alla.	inte	33-37
1	swedish_test_isp_1	Inte	OI	Att upprätthålla säkerheten är inte valfritt, det är en förutsättning för vår verksamhet.	inte	31-35
1	swedish_test_isp_1	Inte	OI	Du behöver inte tveka att fråga om något är oklart.	inte	12-16
1	swedish_test_isp_1	Måste	AA	Detta måste göras för att förhindra obehörig åtkomst.	måste	6-11
1	swedish_test_isp_1	Måste	OI	Varje medarbetare måste vara medveten om sitt ansvar och aktivt bidra till en säker arbetsmiljö.	måste	18-23
1	swedish_test_isp_1	Ska	AA	o Lösenord ska vara komplexa (innehålla stora och små bokstäver, siffror och specialtecken) och bytas regelbundet enligt IT -avdelningens instruktioner.	ska	11-14
1	swedish_test_isp_1	Ska	AA	Besökare ska alltid anmälas och bära synlig besöksbricka.	ska	9-12
1	swedish_test_isp_1	Ska	OI	Denna policy ska utgöra grunden för hur vi skyddar våra informationstillgångar – från kunddata och affärshemligheter till personuppgifter och intern kommunikation.	ska	13-16
1	swedish_test_isp_1	Ska	OI	Informationen ska klassificeras och hanteras enligt företagets interna riktlinjer för dataklassificering och gällande lagstiftning (t.ex.	ska	14-17
1	swedish_test_isp_1	Skall	AA	Detta skall göras för att skydda mot kända sårbarheter.	skall	6-11
1	swedish_test_isp_1	Skall	AA	misstänkt intrång, förlorad utrustning, virusinfektion, misstänkt nätfiske) skall omedelbart rapporteras till IT -avdelningen eller närmaste chef enligt gällande incidenthanteringsrutin.	skall	77-82
1	swedish_test_isp_1	Skall	OI	Granskning och Uppdatering Denna policy skall granskas minst en gång per år, eller oftare vid behov (t.ex.	skall	42-47

2	swedish_test_isp_2	Förbjuden	AA	o Installation av icke -godkänd programvara är förbjuden då den kan introducera sårbarheter som hotar alla våra säkerhetsprinciper.	förbjuden	47-56
2	swedish_test_isp_2	Inte	AA	Operativa Riktlinjer och Ansvar (Dagligt arbete) För att uppfylla våra strategiska mål och principer krävs följande av varje medarbetare i det dagliga arbetet: • 4.1 Användarkonton och Lösenord: o Ditt användarkonto är personligt och får inte delas.	inte	245-249
2	swedish_test_isp_2	Inte	AA	Förvara känsligt material inlåst när det inte används.	inte	42-46
2	swedish_test_isp_2	Inte	AA	o Lagra eller behandla inte företagsinformation på privata enheter eller osäkra molntjänster utan uttryckligt godkännande.	inte	23-27
2	swedish_test_isp_2	Inte	AA	o Säkerställ korrekt radering eller destruktion av information när den inte längre behövs.	inte	71-75
2	swedish_test_isp_2	Inte	OI	Informationssäkerhet är inte bara en teknisk fråga, utan en strategisk grundpelare för att bygga och bibehålla detta förtroende, skydda vårt varumärke och säkerställa vår långsiktiga konkurrenskraft och framgång.	inte	24-28
2	swedish_test_isp_2	Inte	OI	Flexibilitet får inte ske på bekostnad av säkerhet.	inte	17-21
2	swedish_test_isp_2	Inte	OI	Bristande efterlevnad ri skerar inte bara operativa störningar utan kan allvarligt skada företagets strategiska tillgångar som varumärke och kundförtroende.	inte	32-36
2	swedish_test_isp_2	Ska	AA	virus, dataintrång, förlorad utrustning, misstänkt obehörig åtkomst) ska omedelbart rapporteras till IT -avdelningen eller närmaste chef enligt gällande rutin.	ska	70-73
2	swedish_test_isp_2	Ska	OI	Vårt långsiktiga mål är att informationssäkerhet ska vara en affärsmöjliggörare , som stödjer innovation och effektivitet utan att kompromissa med skyddet av våra värdefulla tillgångar.	ska	49-52
2	swedish_test_isp_2	Ska	OI	Grundläggande Säkerhetsprinciper (Strategisk grund för operationella regler) All hantering av information och system inom Exempelföretaget ABC ska vägledas av följande principer: • Konfidentialitet: Information ska endast vara tillgänglig för behöriga individer.	ska	145-148
2	swedish_test_isp_2	Ska	OI	Grundläggande Säkerhetsprinciper (Strategisk grund för operationella regler) All hantering av information och system inom Exempelföretaget ABC ska vägledas av följande principer: • Konfidentialitet: Information ska endast vara tillgänglig för behöriga individer.	ska	216-219
2	swedish_test_isp_2	Ska	OI	• Riktighet (Integritet): Information ska vara korrekt, fullständig och skyddad mot otillåten ändring eller radering.	ska	39-42
2	swedish_test_isp_2	Ska	OI	• Tillgänglighet: Information och tillhörande system ska vara tillgängliga för behöriga användare när de behövs.	ska	54-57
2	swedish_test_isp_2	Ska	OI	• Minsta möjliga behörighet: Användare ska endast tilldelas de behörigheter som är nödvändiga för att utföra sina arbetsuppgifter.	ska	40-43
2	swedish_test_isp_2	Ska	OI	• Riskbaserat förhållningssätt: Säkerhetsåtgärder ska baseras på en bedömning av risker och anpassas efter informationens värde och känslighet.	ska	51-54
2	swedish_test_isp_2	Ska	OI	• Ansvarsskyldighet: Alla handlingar ska kunna spåras till en ansvarig individ eller process.	ska	38-41
2	swedish_test_isp_2	Ska	OI	Policyöversyn och Kontinuerlig Förbättring Denna policy ska ses över minst årligen, eller vid behov, av ansvarig funktion (t.ex.	ska	58-61