					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: PII14					Titlu tad-dokument: **Politika dwar is-Sigurtà tal-PII u l-Kontroll tal-Aċċess**							
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025			Sid tad-dokument:							
X	Politika		Standard		Proċedura		Formola		Reġistru		Oħra	

Storja tar-reviżjonijiet				
Numru tar-reviżjoni	**Data tar-reviżjoni**	**Bidliet**	**Ivrevedut minn**	**Sid tal-proċess**

Approvazzjonijiet			
Isem	**Pożizzjoni**	**Data**	**Firma**

Allinjata ma' standards u regolamenti

Standard / Regolament	Klawżola / Kontroll / Artikolu	Applikabbiltà	Tip ta' kopertura	Kumment
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Ippjanar u tħaddim tal-kontrolli tas-sigurtà tal-PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Evidenza, monitoraġġ u azzjoni korrettiva
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identità u drittijiet tal-aċċess għall-ipproċessar tal-PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Protezzjoni tal-endpoint u awtentikazzjoni sigura
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logging u protezzjoni kriptografika
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Sigurtà tal-applikazzjonijiet u arkitettura sigura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Protezzjoni u rieżami tar-reġistri
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Sigurtà, responsabbiltà u kontrolli tal-proċessur
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integrazzjoni tal-kontrolli tal-ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Gwida għall-implimentazzjoni tal-kontrolli tas-sigurtà
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Prinċipji tas-sigurtà tal-informazzjoni u tal-konformità mal-privatezza
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4;	Both	Supporting	Kontrolli tas-sigurtà għall-protezzjoni tal-PII

	Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Kamp ta' applikazzjoni

1.1 Din il-politika tiddefinixxi r-rekwiżiti tas-sigurtà u tal-kontroll tal-aċċess speċifiċi għall-PII għal sistemi, applikazzjonijiet, servizzi, apparati, ambjenti cloud u proċessi operattivi li jaħżnu, jittrażmettu, jipproċessaw, jaċċessaw, jamministraw jew jipproteġu PII.

1.2 Din il-politika tapplika għal kuntesti ta' kontrollur, kontrollur konġunt, proċessur u subproċessur fejn l-organizzazzjoni tiddetermina, tħaddem, tappoġġa jew tiddependi fuq kontrolli tas-sigurtà għall-ipproċessar tal-PII.

1.3 Din il-politika tkopri l-oqsma li ġejjin tal-kontrolli tas-sigurtà tal-PII:

1.3.1 linja bażi tas-sigurtà tal-PII u integrazzjoni ma' politiki eżistenti tas-sigurtà tal-informazzjoni;

1.3.2 kontroll tal-aċċess;

1.3.3 awtentikazzjoni;

1.3.4 aċċess privileġġjat;

1.3.5 iċċifrar u ħażna sigura;

1.3.6 logging u monitoraġġ;

1.3.7 konfigurazzjoni sigura u ġestjoni tal-vulnerabbiltajiet;

1.3.8 kontrolli tal-aċċess għall-endpoints u għall-cloud;

1.3.9 rabta tal-evidenza permezz ta' REG02, REG08, REG10 u REG12.

1.4 Din il-politika ma tissostitwixxix sistema sħiħa ta' ġestjoni tas-sigurtà tal-informazzjoni, politika tas-sigurtà tan-network, politika dwar l-iżvilupp sigur, politika tal-backup, politika tal-endpoint, politika tas-sigurtà tal-cloud, standard kriptografiku, proċedura tal-ġestjoni tal-vulnerabbiltajiet jew proċedura ta' rispons għall-inċidenti. Fejn dawk il-politiki diġà jeżistu, din il-politika tiddefinixxi r-rabta u r-rekwiżiti tal-evidenza speċifiċi għall-PII meħtieġa għall-assigurazzjoni tal-PIMS.

1.5 Din il-politika ma tidduplikax:

1.5.1 l-inventarju tal-ipproċessar tal-PII u s-sjieda tal-bażi legali f'PII03;

1.5.2 il-metodoloġija tar-riskju tal-privatezza u tad-DPIA f'PII07;

1.5.3 il-gates tal-privatezza mid-disinn f'PII08;

1.5.4 ir-regoli dwar il-ġbir, l-użu, l-iżvelar u l-kondiviżjoni f'PII09;

1.5.5 l-eżekuzzjoni taż-żamma, it-tħassir u r-rimi f'PII10;

1.5.6 il-governanza taċ-ċiklu tal-ħajja tal-proċessur f'PII12;

1.5.7 il-kontrolli tal-mekkaniżmu ta' trasferiment internazzjonali f'PII13;

1.5.8 il-fluss tax-xogħol għall-inċidenti u l-ksur f'PII15;

1.5.9 il-governanza tal-informazzjoni dokumentata f'PII17;

1.5.10 il-governanza tal-monitoraġġ, l-awditjar u t-titjib tal-PIMS f'PII18.

1.6 Għal din il-politika, logs operattivi, outputs tal-għodod tas-sigurtà, esportazzjonijiet tar-rieżami tal-aċċess, rapporti tal-vulnerabbiltajiet u evidenza tal-konfigurazzjoni huma sorsi ta' evidenza li jiġu mehmuża ma', imqassra fi, jew referenzjati mill-oġġetti kanoniċi tal-evidenza. Mhumiex reġistri separati tal-PIMS.

2. Għan

2.1 L-għan ta' din il-politika huwa li jiġi żgurat li l-PII tkun protetta permezz ta' kontrolli tas-sigurtà u tal-aċċess xierqa, allinjati mar-riskju u awditabbli matul l-ipproċessar kollu.

2.2 Din il-politika tippermetti lill-organizzazzjoni turi li l-kontrolli tas-sigurtà tal-PII jiġu ppjanati, implimentati, rieżaminati, immonitorjati u mtejba permezz ta' REG02, REG08, REG10 u REG12 mingħajr ma jinħolqu reġistri tas-sigurtà duplikati jew jiġu sostitwiti politiki eżistenti tas-sigurtà tal-informazzjoni.

3. Objettivi

3.1 L-objettivi ta' din il-politika huma li:

3.1.1 tiddefinixxi linja bażi tal-kontroll tal-aċċess għall-PII għas-sistemi u l-attivitajiet tal-ipproċessar;

3.1.2 tiżgura li l-kontrolli tal-awtentikazzjoni jkunu xierqa għas-sensittività u l-kuntest tal-aċċess tal-PII;

3.1.3 tiddefinixxi r-rekwiżiti tar-rieżami għall-aċċess privileġġjat u ordinarju għall-PII;

3.1.4 tiddefinixxi l-aspettattivi tal-iċċifrar u tal-ħażna sigura għall-PII maħżuna, fi tranżitu u f'kuntesti rilevanti tal-cloud jew tal-endpoint;

3.1.5 tiddefinixxi l-aspettattivi tal-logging u tal-monitoraġġ għall-aċċess għal, il-bidliet fi u l-amministrazzjoni tal-PII;

3.1.6 tiddefinixxi r-rekwiżiti tal-evidenza tal-konfigurazzjoni sigura u tal-vulnerabbiltajiet għas-sistemi li jipproċessaw PII;

3.1.7 tiddefinixxi l-aspettattivi tal-aċċess għall-endpoints u għall-cloud mingħajr ma toħloq politika sħiħa tas-sigurtà tal-endpoints jew tal-cloud;

3.1.8 torbot inċidenti suspettati tas-sigurtà tal-PII ma' REG10 mingħajr ma tidduplika l-fluss tax-xogħol tal-inċidenti;

3.1.9 tintegra ma' politiki eżistenti tas-sigurtà tal-informazzjoni fejn disponibbli;

3.1.10 iżżomm evidenza lesta għall-awditjar bl-użu biss ta' REG02, REG08, REG10 u REG12.

4. Dikjarazzjonijiet tal-politika

4.1 Linja bażi tas-sigurtà tal-PII u integrazzjoni mal-ISMS

4.1.1 [Both] The Information Security Lead GĦANDU jiddefinixxi l-linja bażi tas-sigurtà tal-PII għal kull sistema jew servizz li jipproċessa PII f'REG12 qabel ma s-sistema jew is-servizz jidħol fl-ambjent ta' produzzjoni jew jinbidel b'mod materjali.

4.1.2 [Both] The System Owner / Application Owner GĦANDU jirreġistra l-post tal-evidenza tal-kontroll tas-sigurtà tal-PII implimentat f'REG12 qabel ma jiddependi fuq kontroll eżistenti tas-sigurtà tal-informazzjoni għall-assigurazzjoni tal-PIMS.

4.1.3 [Controller] The Process Owner / Business Owner GĦANDU jidentifika s-sensittività tal-PII, il-kuntest tal-ipproċessar u l-ħtieġa ta' aċċess f'REG02 qabel ma jitlob aċċess ġdid jew mibdul b'mod materjali għall-PII.

4.1.4 [Processor] The Vendor / Procurement Owner GĦANDU jirreġistra l-istruzzjonijiet tas-sigurtà tal-klijent, il-konfini tar-responsabbiltà tal-klijent u l-impenji tas-sigurtà tal-proċessur f'REG08 qabel ma jibda jew jinbidel b'mod materjali l-aċċess tal-proċessur għall-PII tal-klijent.

4.1.5 [Both] The Privacy Lead / PIMS Manager GĦANDU jivverifika li l-evidenza tas-sigurtà tal-PII tkun marbuta ma' REG02, REG08, REG10 jew REG12 qabel ma jaċċetta l-attività tal-ipproċessar bħala awditabbli għall-PIMS.

4.2 Linja bażi tal-kontroll tal-aċċess

4.2.1 [Both] The System Owner / Application Owner GĦANDU jirrestriġi l-aċċess għall-PII għal rwoli approvati u utenti awtorizzati rreġistrati jew traċċabbli f'REG02 jew REG12 qabel ma jiġi attivat l-aċċess.

4.2.2 [Both] The Process Owner / Business Owner GĦANDU japprova l-għan tan-negozju għall-aċċess għall-PII f'REG02 jew REG12 qabel ma The System Owner / Application Owner jipprovdi l-aċċess.

4.2.3 [Both] The System Owner / Application Owner GĦANDU jirrieżamina l-aċċess tal-utenti għal sistemi li jipproċessaw PII b'impatt għoli jew sensittiva mill-inqas kull tliet xhur u jirreġistra r-riżultat tar-rieżami f'REG12.

4.2.4 [Both] The System Owner / Application Owner GĦANDU jirrieżamina l-aċċess tal-utenti għal sistemi oħra li jipproċessaw PII mill-inqas darba fis-sena u jirreġistra r-riżultat tar-rieżami f'REG12.

4.2.5 [Both] The System Owner / Application Owner GĦANDU jneħħi jew jemenda l-aċċess għall-PII f'REG12 fi żmien jum ta' xogħol wieħed wara bidla fir-rwol, terminazzjoni, tlestija tal-kuntratt jew meta l-aċċess ma jkunx għadu meħtieġ.

4.2.6 [Processor] The Vendor / Procurement Owner GĦANDU jikkonferma f'REG08 li l-aċċess tal-proċessur għall-PII tal-klijent ikun limitat għall-istruzzjonijiet dokumentati tal-klijent qabel ma l-aċċess jiġi attivat jew mibdul.

4.2.7 [Subprocessor] The Vendor / Procurement Owner GĦANDU jikkonferma f'REG08 li l-aċċess tas-subproċessur għall-PII ikun limitat għal attivitajiet awtorizzati ta' subproċessar qabel ma l-aċċess tas-subproċessur jiġi attivat jew mibdul.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Eċċezzjonijiet

9.1.1 [Both] The Information Security Lead GĦANDU jirreġistra kull eċċezzjoni għal rekwiżit tas-sigurtà tal-PII jew tal-kontroll tal-aċċess f'REG12 qabel ma l-eċċezzjoni tiġi attivata.

9.1.2 [Both] The Data Protection Officer / Privacy Advisor GĦANDU jagħti parir dwar eċċezzjonijiet tas-sigurtà tal-PII ta' riskju ogħla f'REG12 qabel l-approvazzjoni.

9.1.3 [Both] Top Management GĦANDU japprova eċċezzjonijiet tas-sigurtà tal-PII f'REG12 qabel l-attivazzjoni meta l-eċċezzjoni taffettwa PII b'impatt għoli, PII sensittiva, aċċess privileġġjat, iċċifrar, logging jew vulnerabbiltajiet mhux solvuti ta' riskju għoli.

9.1.4 [Both] The Information Security Lead GĦANDU jiddefinixxi d-data tal-iskadenza tal-eċċezzjoni, il-kontroll kumpensatorju u d-data tar-rieżami f'REG12 qabel l-approvazzjoni tal-eċċezzjoni.

9.1.5 [Both] The System Owner / Application Owner GĦANDU jirrimedja, iġedded jew jagħlaq eċċezzjonijiet skaduti tas-sigurtà tal-PII f'REG12 fi żmien ħamest ijiem ta' xogħol wara l-iskadenza.

9.1.6 [Processor] The Vendor / Procurement Owner GĦANDU jirreġistra eċċezzjonijiet tas-sigurtà tal-proċessur jew tas-subproċessur li jaffettwaw il-PII tal-klijent f'REG08 u REG12 qabel l-aċċettazzjoni.

10. Applikazzjoni

10.1.1 [Both] The Privacy Lead / PIMS Manager GĦANDU jirreġistra nuqqasijiet ta' konformità għal evidenza tas-sigurtà tal-PII nieqsa jew mhux kompluta f'REG12 fi żmien ħamest ijiem ta' xogħol mill-identifikazzjoni.

10.1.2 [Both] The Information Security Lead GĦANDU jassenja s-sjieda tar-rimedjazzjoni għall-fallimenti tal-kontrolli tas-sigurtà tal-PII f'REG12 fi żmien ħamest ijiem ta' xogħol mill-verifika.

10.1.3 [Both] The System Owner / Application Owner GĦANDU jiddiżattiva jew jirrestrinġi aċċess mhux awtorizzat, eċċessiv jew mhux sostnut għall-PII fi żmien jum ta' xogħol wieħed mill-verifika u jirreġistra l-azzjoni f'REG12.

10.1.4 [Conditional] The Incident Response Coordinator GĦANDU jorbot azzjonijiet ta' applikazzjoni ma' REG10 fi żmien jum ta' xogħol wieħed meta l-kwistjoni tal-applikazzjoni tinvolvi inċident suspettat jew ikkonfermat tal-PII.

10.1.5 [Both] Top Management GĦANDU jirrieżamina nuqqasijiet ta' konformità ripetuti jew ta' riskju għoli tas-sigurtà tal-PII f'REG12 qabel ir-rieżami mill-maniġment.

11. Rieżami u manutenzjoni

11.1.1 [All] The Privacy Lead / PIMS Manager GĦANDU jirrieżamina din il-politika ma' The Information Security Lead mill-inqas darba fis-sena u jirreġistra r-riżultat tar-rieżami f'REG12.

11.1.2 [Both] The Information Security Lead GĦANDU jirrieżamina l-linja bażi tas-sigurtà tal-PII f'REG12 fi żmien 30 jum wara bidla materjali teknoloġika, fit-theddid, fl-awditjar, f'inċident jew regolatorja li taffettwa s-sigurtà tal-PII.

11.1.3 [Both] The System Owner / Application Owner GĦANDU jaġġorna l-evidenza tas-sigurtà tal-PII fil-livell tas-sistema f'REG12 fi żmien 30 jum wara bidla materjali fl-arkitettura, fl-aċċess, fil-konfigurazzjoni, fil-vulnerabbiltajiet jew fil-logging.

11.1.4 [Processor] The Vendor / Procurement Owner GĦANDU jirrieżamina l-evidenza tar-responsabbiltajiet tas-sigurtà tal-PII tal-proċessuri u tas-subproċessuri f'REG08 fi żmien 30 jum wara bidla materjali fis-servizz, fl-istruzzjoni tal-klijent jew fis-subproċessur.

11.1.5 [All] The Internal Audit / Compliance Reviewer GĦANDU jivverifika l-evidenza tar-rieżami tal-politika u evidenza magħżula tal-kontrolli tas-sigurtà tal-PII f'REG12 skont il-pjan tal-awditjar approvat.

12. Politiki relatati

12.1 Din il-politika għandha tinqara flimkien ma':

12.1.1 PII01 - Politika tas-Sistema ta' Ġestjoni tal-Informazzjoni dwar il-Privatezza;

12.1.2 PII02 - Politika dwar ir-Rwoli, ir-Responsabbiltajiet u r-Responsabbiltà tal-Privatezza;

12.1.3 PII03 - Politika dwar l-Inventarju tal-Ipproċessar tal-PII u l-Bażi Legali;

12.1.4 PII07 - Politika dwar il-Valutazzjoni tar-Riskju tal-Privatezza u d-DPIA;

12.1.5 PII08 - Politika dwar il-Privatezza mid-Disinn u b'mod Predefinit;

12.1.6 PII09 - Politika dwar il-Ġbir, l-Użu, l-Iżvelar u l-Kondiviżjoni tal-PII;

12.1.7 PII10 - Politika dwar iż-Żamma, it-Tħassir u r-Rimi tal-PII;

12.1.8 PII12 - Politika dwar il-Ġestjoni tal-Privatezza tal-Proċessuri, tas-Subproċessuri u tal-Partijiet Terzi;

12.1.9 PII13 - Politika dwar it-Trasferiment Internazzjonali tal-PII;

12.1.10 PII15 - Politika dwar il-Ġestjoni tal-Inċidenti u l-Ksur tal-PII;

12.1.11 PII16 - Politika dwar it-Taħriġ, is-Sensibilizzazzjoni u l-Kompetenza fil-Privatezza;

12.1.12 PII17 - Politika dwar il-Ġestjoni tal-Informazzjoni Dokumentata u l-Evidenza tal-PIMS;

12.1.13 PII18 - Politika dwar il-Monitoraġġ, l-Awditjar u t-Titjib tal-PIMS.

13. Standards u oqfsa ta' referenza

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].