

ÍST ISO/IEC 17799:2005

Gildistaka 2006-07-15

ICS 35.040

**Upplýsingatækni –
Öryggisækni –
Starfsvenjur fyrir stjórnun
upplýsingaöryggis**

**Information technology –
Security techniques –
Code of practice for information
security management**

ÍST ISO/IEC 17799:2005

© Staðlaráð Íslands 2006. Öll réttindi áskilin.

Án skriflegs leyfis útgefanda má ekki endurprenta eða afrita þennan staðal með neinum hætti, vélrænum eða rafrænum, svo sem ljósritun, hljóðritun eða annarri aðferð sem nú er þekkt eða verður síðar fundin upp, né miðla staðlinum í rafrænu gagnasafni.

1. prentun.

Formáli íslensku þýðingarinnar

Þessi íslenski staðall, ÍST ISO/IEC 17799:2005, sem einnig er alþjóðlegur staðall, var staðfestur af Staðlaráði Íslands, sem er samstarfsvettvangur íslenskra hagsmunaaðila til að vinna að stöðlun og beitingu staðla. Íslenska þýðingin var gerð að tilhlutan Staðlaráðs Íslands og FUT.

Vinnuhópur á vegum Fagráðs í upplýsingatækni (FUT), sem starfar á vegum Staðlaráðs Íslands, vann að þýðingu staðalsins og fá meðlimir vinnuhópsins þakkir fyrir vinnu við yfirlestur og ráðgjöf.

Vinnuhópurinn skipaðu:

Marinó G. Njálsson
Jónas Sturla Sverrisson
Elías Atlason
Kristín Þórsdóttir
Sigurjón Þór Árnason
Þorvarður Kári Ólafsson
Guðbjörg Björnsdóttir (Staðlaráði/FUT)
Stefán Briem (þýðandi)

Þessi önnur útgáfa er uppfærsla á fyrstu útgáfunni (ISO/IEC 17799:2000) og inniheldur all nokkrar breytingar og viðbætur.

Þýðingin er einungis gerð til hagræðis fyrir íslenska notendur. Kappkostað hefur verið að hafa íslenska textann eins nákvæman og framast er unnt. Engu að síður getur Staðlaráð Íslands ekki ábyrgst að þýðingin endurspegli nákvæmlega merkingu frumtextans, orð fyrir orð.

Af þessum sökum er enski textinn birtur við hlið hins íslenska og til hans ber að leita komi til deilumála um túlkun ákvæða í staðlinum. Staðlarnir eru í stöðugri endurskoðun og þar með íslenska þýðingin. Notendur staðlanna eru eindregið hvattir til að koma athugasemdum og ábendingum til Staðlaráðs Íslands.

Vinnuhópurinn taldi rétt að gefa skýringu á notkun hugtaksins „organization“ sem þýtt er með orðinu „fyrirtæki“.

Þessi notkun orðsins er viðtekin í öðrum stöðlum (t.d. ÍST EN ISO 9000:2005) og hefur hlotið góðan hljómgrunn.

Með „fyrirtæki“ er átt við t.d. félag, hlutafélag, firma, atvinnufyrirtæki, stofnun, góðgerðastofnun, einyrkja, samtök eða hluta eða samsetningu af þessu.

Fyrirtæki getur verið opinbert eða í einkaeign.

ÍST ISO/IEC 17799:2005

Efnisyfirlit

Formáli	11
0 Inngangur	12
0.1 Hvað er upplýsingaöryggi?	12
0.2 Af hverju þörf er á upplýsingaöryggi?	12
0.3 Hvernig koma á upp öryggiskröfum	13
0.4 Að meta öryggisáhættu	13
0.5 Val á stýringum	14
0.6 Upphafsréitur upplýsingaöryggis	14
0.7 Þættir sem ráða úrslitum um árangur	15
0.8 Þróun eigin leiðbeininga	16
1 Umfang	17
2 Hugtök og skilgreiningar	18
3 Skipulag þessa staðals	21
3.1 Greinar	21
3.2 Meginflokkar öryggis	21
4 Áhættumat og -meðferð	23
4.1 Mat á öryggisáhættu	23
4.2 Meðferð öryggisáhættu	23
5 Öryggisstefna	25
5.1 Upplýsingaöryggisstefna	25
5.1.1 Skjalfest upplýsingaöryggisstefna	25
5.1.2 Rýni á upplýsingaöryggisstefnunni	26
6 Skipulag upplýsingaöryggis	28
6.1 Innra skipulag	28
6.1.1 Skuldbinding stjórnenda vegna upplýsingaöryggis	28
6.1.2 Samhæfing upplýsingaöryggis	29
6.1.3 Úthlutun ábyrgðar á upplýsingaöryggi	30
6.1.4 Heimilunarferli fyrir upplýsingavinnslubúnað	31
6.1.5 Trúnaðarsamningar	31
6.1.6 Tengsl við yfirvöld	32
6.1.7 Tengsl við sérstaka hagsmunahópa	33

Contents

Foreword	11
0 Introduction	12
0.1 What is information security?	12
0.2 Why information security is needed?	12
0.3 How to establish security requirements	13
0.4 Assessing security risks	13
0.5 Selecting controls	14
0.6 Information security starting point	14
0.7 Critical success factors	15
0.8 Developing your own guidelines	16
1 Scope	17
2 Terms and definitions	18
3 Structure of this standard	21
3.1 Clauses	21
3.2 Main security categories	21
4 Risk assessment and treatment	23
4.1 Assessing security risks	23
4.2 Treating security risks	23
5 Security policy	25
5.1 Information security policy	25
5.1.1 Information security policy document	25
5.1.2 Review of the information security policy	26
6 Organization of information security	28
6.1 Internal organization	28
6.1.1 Management commitment to information security	28
6.1.2 Information security co-ordination	29
6.1.3 Allocation of information security responsibilities	30
6.1.4 Authorization process for information processing facilities	31
6.1.5 Confidentiality agreements	31
6.1.6 Contact with authorities	32
6.1.7 Contact with special interest groups	33

6.1.8	Sjálfstæð rýni á upplýsingaöryggi	33	6.1.8	Independent review of information security	33
6.2	Utanaðkomandi aðilar	35	6.2	External parties	35
6.2.1	Ákvörðun áhættu sem tengist utanaðkomandi aðilum	35	6.2.1	Identification of risks related to external parties	35
6.2.2	Öryggiskröfur í samskiptum við viðskiptavinum	37	6.2.2	Addressing security when dealing with customers	39
6.2.3	Öryggiskröfur í samningum við þriðju aðila	39	6.2.3	Addressing security in third party agreements	39
7	Eignastjórnun	43	7	Asset management	43
7.1	Ábyrgð á eignum	43	7.1	Responsibility for assets	43
7.1.1	Eignaskrá	43	7.1.1	Inventory of assets	43
7.1.2	Forsjá eigna	44	7.1.2	Ownership of assets	44
7.1.3	Ásættanleg notkun eigna	45	7.1.3	Acceptable use of assets	45
7.2	Flokkun upplýsinga	45	7.2	Information classification	45
7.2.1	Leiðbeiningar um flokkun	45	7.2.1	Classification guidelines	45
7.2.2	Merkingar og meðferð upplýsinga	46	7.2.2	Information labeling and handling	46
8	Mannauðsöryggi	48	8	Human resources security	48
8.1	Áður en gengið er frá ráðningu	48	8.1	Prior to employment	48
8.1.1	Hlutverk og ábyrgð	48	8.1.1	Roles and responsibilities	48
8.1.2	Ferilkönnun	49	8.1.2	Screening	49
8.1.3	Ráðningarskilmálar	50	8.1.3	Terms and conditions of employment	50
8.2	Meðan ráðning er í gildi	51	8.2	During employment	51
8.2.1	Ábyrgð stjórnenda	51	8.2.1	Management responsibilities	51
8.2.2	Vitund, fræðsla og þjálfun í upplýsingaöryggi	52	8.2.2	Information security awareness, education, and training	52
8.2.3	Agæferli	53	8.2.3	Disciplinary process	53
8.3	Lok eða breyting á ráðningu	54	8.3	Termination or change of employment	54
8.3.1	Ábyrgð við ráðningarlok	54	8.3.1	Termination responsibilities	54
8.3.2	Eignum skilað	55	8.3.2	Return of assets	55
8.3.3	Niðurfelling aðgangsréttinda	55	8.3.3	Removal of access rights	55
9	Raunlægt öryggi og umhverfisöryggi	57	9	Physical and environmental security	57
9.1	Örugg svæði	57	9.1	Secure areas	57
9.1.1	Öryggismæri	57	9.1.1	Physical security perimeter	57
9.1.2	Inngangsvarsla	58	9.1.2	Physical entry controls	58
9.1.3	Skrifstofur, herbergi og búnaður gerð örugg	59	9.1.3	Securing offices, rooms, and facilities	59
9.1.4	Vernd gegn utanaðkomandi ógnum og umhverfisógnum	59	9.1.4	Protecting against external and environmental threats	59
9.1.5	Vinna á öruggum svæðum	60	9.1.5	Working in secure areas	60

ÍST ISO/IEC 17799:2005

9.1.6 Svæði fyrir almennan aðgang, dreifingu og lestun _____	60	9.1.6 Public access, delivery, and loading areas _____	60
9.2 Öryggi tækjabúnaðar _____	61	9.2 Equipment security _____	61
9.2.1 Staðsetning og verndun tækjabúnaðar _____	61	9.2.1 Equipment siting and protection _____	61
9.2.2 Stoðveitur _____	62	9.2.2 Supporting utilities _____	62
9.2.3 Öryggi raflagna _____	63	9.2.3 Cabling security _____	63
9.2.4 Viðhald tækjabúnaðar _____	64	9.2.4 Equipment maintenance _____	64
9.2.5 Öryggi tækjabúnaðar utan starfssvæðis _____	65	9.2.5 Security of equipment off-premises _____	65
9.2.6 Örugg förgun eða endurnýting tækjabúnaðar _____	66	9.2.6 Secure disposal or re-use of equipment _____	66
9.2.7 Brottflutningur eigna _____	66	9.2.7 Removal of property _____	66
10 Stjórnun á samskiptum og rekstri _____	68	10 Communications and operations management _____	68
10.1 Verklagsreglur um rekstur og ábyrgð á rekstri _____	68	10.1 Operational procedures and responsibilities _____	68
10.1.1 Skjalfestar verklagsreglur um rekstur _____	68	10.1.1 Documented operating procedures _____	68
10.1.2 Breytingastjórnun _____	69	10.1.2 Change management _____	69
10.1.3 Aðskilnaður skylduverka _____	70	10.1.3 Segregation of duties _____	70
10.1.4 Aðskilnaður milli þróunar-, prófunar- og rekstrarbúnaðar _____	70	10.1.4 Separation of development, test, and operational facilities _____	70
10.2 Stjórnun á afhendingu þjónustu þriðju aðila _____	71	10.2 Third party service delivery management _____	71
10.2.1 Afhending þjónustu _____	71	10.2.1 Service delivery _____	71
10.2.2 Vöktun og rýni á þjónustu þriðju aðila _____	72	10.2.2 Monitoring and review of third party services _____	72
10.2.3 Stjórnun á breytingum þjónustu þriðju aðila _____	73	10.2.3 Managing changes to third party services _____	73
10.3 Skipulagning kerfa og samþykki á kerfum _____	74	10.3 System planning and acceptance _____	74
10.3.1 Gerð áætlana um afkastagetu _____	74	10.3.1 Capacity management _____	74
10.3.2 Samþykki á kerfum _____	74	10.3.2 System acceptance _____	74
10.4 Vernd gegn spillikóta og farandkóta _____	76	10.4 Protection against malicious and mobile code _____	76
10.4.1 Stýringar gegn spillikóta _____	76	10.4.1 Controls against malicious code _____	76
10.4.2 Stýringar gegn farandkóta _____	77	10.4.2 Controls against mobile code _____	77
10.5 Öryggisafritun _____	78	10.5 Back-up _____	78
10.5.1 Öryggisafritun upplýsinga _____	78	10.5.1 Information back-up _____	78
10.6 Stjórnun netöryggis _____	80	10.6 Network security management _____	80
10.6.1 Netstýringar _____	81	10.6.1 Network controls _____	81
10.6.2 Öryggi í netþjónustu _____	81	10.6.2 Security of network services _____	81
10.7 Meðferð miðla _____	82	10.7 Media handling _____	82
10.7.1 Umsjón með færanlegum miðlum _____	82	10.7.1 Management of removable media _____	82

10.7.2 Förgun miðla _____	82	10.7.2 Disposal of media _____	82
10.7.3 Verklagsreglur um meðferð upplýsinga _____	83	10.7.3 Information handling procedures _____	83
10.7.4 Öryggi kerfisskjala _____	84	10.7.4 Security of system documentation _____	84
10.8 Skipti á upplýsingum _____	84	10.8 Exchange of information _____	84
10.8.1 Stefna og verklagsreglur um skipti á upplýsingum _____	85	10.8.1 Information exchange policies and procedures _____	85
10.8.2 Samningar um skipti _____	87	10.8.2 Exchange agreements _____	87
10.8.3 Raunlægir miðlar í flutningi _____	88	10.8.3 Physical media in transit _____	88
10.8.4 Rafrænar skeytasendingar _____	89	10.8.4 Electronic messaging _____	89
10.8.5 Rekstrarleg upplýsingakerfi _____	89	10.8.5 Business information systems _____	89
10.9 Rafræn viðskiptaþjónusta _____	90	10.9 Electronic commerce services _____	90
10.9.1 Rafræn viðskipti _____	91	10.9.1 Electronic commerce _____	91
10.9.2 Netviðskipti _____	92	10.9.2 On-Line Transactions _____	91
10.9.3 Upplýsingar með almennan aðgang _____	93	10.9.3 Publicly available information _____	93
10.10 Vöktun _____	94	10.10 Monitoring _____	94
10.10.1 Úttektarskráning _____	94	10.10.1 Audit logging _____	94
10.10.2 Vöktun á kerfisnotkun _____	95	10.10.2 Monitoring system use _____	95
10.10.3 Verndun dagbókarupplýsinga _____	97	10.10.3 Protection of log information _____	97
10.10.4 Dagbækur kerfisstjóra og rekstrarstjóra _____	97	10.10.4 Administrator and operator logs _____	97
10.10.5 Skráning á villum í dagbækur _____	98	10.10.5 Fault logging _____	98
10.10.6 Samstilling klukkna _____	98	10.10.6 Clock synchronization _____	98
11 Aðgangsstýring _____	100	11 Access control _____	100
11.1 Rekstrarkröfur um aðgangsstýringu _____	100	11.1 Business requirement for access control _____	100
11.1.1 Stefna um aðgangsstýringu _____	100	11.1.1 Access control policy _____	100
11.2 Stýring á aðgangi notenda _____	101	11.2 User access management _____	101
11.2.1 Notendaskráning _____	102	11.2.1 User registration _____	102
11.2.2 Sérreittindastýring _____	103	11.2.2 Privilege management _____	103
11.2.3 Stýring á aðgangsorðum notenda _____	103	11.2.3 User password management _____	103
11.2.4 Rýni á aðgangsréttindum notenda _____	104	11.2.4 Review of user access rights _____	104
11.3 Ábyrgð notenda _____	105	11.3 User responsibilities _____	105
11.3.1 Notkun aðgangsorða _____	105	11.3.1 Password use _____	105
11.3.2 Eftirlitslaus notendabúnaður _____	106	11.3.2 Unattended user equipment _____	106
11.3.3 Stefna um að ekkert sé skilið eftir á glámbekk _____	107	11.3.3 Clear desk and clear screen policy _____	107
11.4 Stýring á netaðgangi _____	108	11.4 Network access control _____	108
11.4.1 Stefna um notkun netþjónustu _____	108	11.4.1 Policy on use of network services _____	108
11.4.2 Sannvottun notenda ytri tengingar _____	109 110	11.4.2 User authentication for external connections _____	109 110
11.4.3 Kennsl borin á tækjabúnað í netum _____	110	11.4.3 Equipment identification in networks _____	110

ÍST ISO/IEC 17799:2005

11.4.4 Verndun fjartengdra greiningar- og samstillingartengja _____	110	11.4.4 Remote diagnostic and configuration port protection ____	110
11.4.5 Aðskilnaður innan neta _____	111	11.4.5 Segregation in networks _____	111
11.4.6 Eftirlit með nettengingum _____	112	11.4.6 Network connection control ____	112
11.4.7 Stýring á netbeiningu _____	112	11.4.7 Network routing control _____	112
11.5 Stýring á aðgangi að stýrikerfi _____	113	11.5 Operating system access control ____	113
11.5.1 Öruggar innskráningaraðferðir ____	114	11.5.1 Secure log-on procedures ____	114
11.5.2 Notandakenni og sannvottun ____	115	11.5.2 User identification and authentication _____	115
11.5.3 Aðgangsorðakerfi _____	116	11.5.3 Password management system _	116
11.5.4 Notkun kerfishjálparforrita _____	117	11.5.4 Use of system utilities _____	117
11.5.5 Tímalokun starfslota _____	117	11.5.5 Session time-out _____	117
11.5.6 Takmörkun tengitíma _____	118	11.5.6 Limitation of connection time ____	118
11.6 Stýring á aðgangi að hugbúnaði og upplýsingum _____	119	11.6 Application and information access control _____	119
11.6.1 Takmörkun á aðgangi að upplýsingum _____	119	11.6.1 Information access restriction ____	119
11.6.2 Einangrun viðkvæmra kerfa ____	120	11.6.2 Sensitive system isolation _____	120
11.7 Farandvinnsla og fjarvinna _____	120	11.7 Mobile computing and teleworking ____	120
11.7.1 Farandvinnsla og samskipti ____	120	11.7.1 Mobile computing and communications _____	120
11.7.2 Fjarvinna _____	122	11.7.2 Teleworking _____	122
12 Öflun, þróun og viðhald upplýsingakerfa ____	124	12 Information systems acquisition, development and maintenance _____	124
12.1 Öryggiskröfur vegna upplýsingakerfa ____	124	12.1 Security requirements of information systems _____	124
12.1.1 Greining og framsetning á öryggiskröfum _____	125	12.1.1 Security requirements analysis and specification _____	125
12.2 Rétt vinnsla í hugbúnaði _____	125	12.2 Correct processing in applications _____	125
12.2.1 Fullgilding ílagsgagna _____	126	12.2.1 Input data validation _____	126
12.2.2 Stýring á innri vinnslu _____	127	12.2.2 Control of internal processing ____	127
12.2.3 Réttleiki skeyta _____	128	12.2.3 Message integrity _____	128
12.2.4 Fullgilding frálagsgagna _____	128	12.2.4 Output data validation _____	128
12.3 Dulritunarstýringar _____	128	12.3 Cryptographic controls _____	128
12.3.1 Stefna um notkun dulritunar- stýringa _____	130	12.3.1 Policy on the use of cryptographic controls _____	130
12.3.2 Umsjón með lykllum _____	132	12.3.2 Key management _____	132
12.4 Öryggi kerfisskráa _____	132	12.4 Security of system files _____	132
12.4.1 Stýring á rekstrarhugbúnaði ____	133	12.4.1 Control of operational software _	133
12.4.2 Verndun prófunargagna kerfis ____	134	12.4.2 Protection of system test data ____	134
12.4.3 Stýring á aðgangi að frumkóta forrita _____	135	12.4.3 Access control to program source code _____	135

12.5 Öryggi í þróunar- og stuðningsferlum ____	135	12.5 Security in development and support processes _____	135
12.5.1 Verklagsreglur um stýringu á breytingum _____	135	12.5.1 Change control procedures _____	135
12.5.2 Tæknileg rýni á hugbúnaði eftir breytingar á stýrikerfi _____	137	12.5.2 Technical review of applications after operating system changes _	137
12.5.3 Takmarkanir á breytingum á hugbúnaðarpökkum _____	137	12.5.3 Restrictions on changes to software packages _____	137
12.5.4 Upplýsingaleki _____	138	12.5.4 Information leakage _____	138
12.5.5 Útvistuð hugbúnaðarþróun _____	139	12.5.5 Outsourced software development	139
12.6 Stjórnun tækniveila _____	139	12.6 Technical vulnerability management ____	139
12.6.1 Stýring á tækniveilum _____	139	12.6.1 Control of technical vulnerabilities _____	139
13 Umsjón með upplýsingaöryggisatvikum _____	142	13 Information security incident management ____	142
13.1 Skýrslugjöf um atburði og veikleika sem tengjast upplýsingaöryggi _____	142	13.1 Reporting information security events and weaknesses _____	142
13.1.1 Skýrslugjöf um upplýsingaöryggisatburði _____	142	13.1.1 Reporting information security events _____	142
13.1.2 Skýrslugjöf um öryggisveikleika _	144	13.1.2 Reporting security weaknesses _	144
13.2 Stjórnun á upplýsingaöryggisatvikum og -umbótum _____	144	13.2 Management of information security incidents and improvements _____	144
13.2.1 Ábyrgð og verklagsreglur _____	144	13.2.1 Responsibilities and procedures	144
13.2.2 Að læra af upplýsingaöryggisatvikum _____	146	13.2.2 Learning from information security incidents _____	146
13.2.3 Öflun sönnunargagna _____	146	13.2.3 Collection of evidence _____	146
14 Stjórnun á rekstrarsamfellu _____	149	14 Business continuity management _____	149
14.1 Þættir upplýsingaöryggis í stjórnun á rekstrarsamfellu _____	149	14.1 Information security aspects of business continuity management ____	149
14.1.1 Að fella upplýsingaöryggi inn í stjórnunarferli fyrir rekstrarsamfellu _____	149	14.1.1 Including information security in the business continuity management process _____	149
14.1.2 Rekstrarsamfella og áhættumat _	150	14.1.2 Business continuity and risk assessment _____	150
14.1.3 Þróun og innleiðing áætlana um rekstrarsamfellu sem taka til upplýsingaöryggis _____	151	14.1.3 Developing and implementing continuity plans including information security _____	151
14.1.4 Rammi fyrir gerð áætlana um rekstrarsamfellu _____	152	14.1.4 Business continuity planning framework _____	152
14.1.5 Prófun, viðhald og endurmat á áætlunum um rekstrarsamfellu ____	154	14.1.5 Testing, maintaining and re-assessing business continuity plans _____	154

ÍST ISO/IEC 17799:2005

15	Hlíting	156	15	Compliance	156
15.1	Hlíting við réttarfarsákvæði	156	15.1	Compliance with legal requirements	156
15.1.1	Borin kennsl á viðeigandi ákvæði	156	15.1.1	Identification of applicable legislation	156
15.1.2	Hugverkaréttur	156	15.1.2	Intellectual property rights (IPR)	156
15.1.3	Verndun á skráum fyrirtækisins	158	15.1.3	Protection of organizational records	158
15.1.4	Gagnavernd og friðhelgi persónuupplýsinga	159	15.1.4	Data protection and privacy of personal information	159
15.1.5	Að koma í veg fyrir misnotkun upplýsingavinnslubúnaðar	160	15.1.5	Prevention of misuse of information processing facilities	160
15.1.6	Setning reglna um dulritun	161	15.1.6	Regulation of cryptographic controls	161
15.2	Hlíting við öryggisstefnur og -staðla og tæknileg hlíting	161	15.2	Compliance with security policies and standards, and technical compliance	161
15.2.1	Hlíting við öryggisstefnur og -staðla	161	15.2.1	Compliance with security policies and standards	161
15.2.2	Könnun á tæknilegri hlítingu	162	15.2.2	Technical compliance checking	162
15.3	Athugunarefni vegna úttekta á upplýsingakerfum	163	15.3	Information systems audit considerations	163
15.3.1	Stýring úttekta á upplýsingakerfum	163	15.3.1	Information systems audit controls	163
15.3.2	Verndun búnaðar til úttekta á upplýsingakerfum	164	15.3.2	Protection of information systems audit tools	164
Ritaskrá		165	Bibliography		165
Atriðisorðaskrá		167	Index		167

Formáli

ISO (International Organization for Standardization – Alþjóðlegu staðlasamtökin) og IEC (International Electrotechnical Commission – Alþjóða raftækniráðið) mynda sérhæft kerfi fyrir alþjóðlega stöðlun. Staðlastofnanir einstakra landa sem eiga aðild að ISO eða IEC taka þátt í þróun alþjóðastaðla með starfrækslu tækninefnda sem hvor staðlasamtökin um sig setja á fót til að fást við afmörkuð tæknisvið. Tækninefndir ISO og IEC hafa samvinnu um efnissvið sem hagsmunir þeirra beggja tengjast. Aðrar alþjóðlegar stofnanir, bæði þær sem starfa á vegum ríkisstjórna og aðrar, taka einnig þátt, í samvinnu við ISO og IEC. Á sviði upplýsingatækni hafa ISO og IEC komið á fót sameiginlegri tækninefnd, ISO/IEC JTC 1.

Alþjóðastaðlar eru samdir í samræmi við Vinnureglur ISO/IEC, 2. hluta.

Meginverkefni sameiginlegu tækninefndarinnar er að semja alþjóðastaðla. Frumvörp að alþjóðastöðlum, sem sameiginlega tækninefndin hefur komið sér saman um, eru send aðilum samtakanna til atkvæðagreiðslu. Alþjóðastaðall er ekki gefinn út nema að minnsta kosti 75 % þeirra aðila sem greiða atkvæði hafi samþykkt staðalinn.

Athygli er vakin á því að sum atriði í þessu skjali gætu fallið undir einkaleyfi. ISO og IEC bera ekki ábyrgð á að tilgreina einhver eða öll slík einkaleyfi.

Alþjóðastaðallinn ISO/IEC 17799 var saminn af sameiginlegu tækninefndinni ISO/IEC JTC 1, Information technology, undirnefnd SC 27, IT Security techniques.

Þessi önnur útgáfa kemur í stað fyrstu útgáfunnar (ISO/IEC 17799:2000) sem er þar með felld úr gildi en hún hefur verið endurskoðuð tæknilega.

Innan ISO/IEC JTC 1/SC 27 er verið að þróa samstæðu af alþjóðastöðlum á sviði stjórnkerfis upplýsingaöryggis (ISMS). Í samstæðunni eru alþjóðastaðlar um upplýsingaöryggisstjórnun, áhættustjórnun, mælikvarðar og mælingar og leiðbeiningar um innleiðingu. Fyrir þessa samstæðu verður tekið upp númerakerfi með númerum frá 27000.

Lagt er til að frá árinu 2007 verði þessi nýja útgáfa af ISO/IEC 17799 sett inn í nýja númerakerfið sem ISO/IEC 27002.

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 17799 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

This second edition cancels and replaces the first edition (ISO/IEC 17799:2000), which has been technically revised.

A family of Information Security Management System (ISMS) International Standards is being developed within ISO/IEC JTC 1/SC 27. The family includes International Standards on information security management system requirements, risk management, metrics and measurement, and implementation guidance. This family will adopt a numbering scheme using the series of numbers 27000 et seq.

From 2007, it is proposed to incorporate the new edition of ISO/IEC 17799 into this new numbering scheme as ISO/IEC 27002.

ÍST ISO/IEC 17799:2005

0 Inngangur

0.1 Hvað er upplýsingaöryggi?

Upplýsingar eru eignir og eins og aðrar mikilvægar rekstrarlegar eignir eru þær ómissandi fyrir rekstur fyrirtækis og þurfa því viðeigandi vernd. Þetta er sérstaklega mikilvægt í rekstrarumhverfi með síauknum innbyrðis tengingum. Í kjölfar þessarar aukningar á innbyrðis tengingum eru upplýsingar berskjaldaðri fyrir sífellt fleiri og margvíslegri ógnum og veilum (sjá einnig OECD Guidelines for the Security of Information Systems and Networks).

Upplýsingar geta verið á margs konar formi. Þær geta verið prentaðar eða ritaðar á pappír, geymdar með rafrænum hætti, sendar með pósti eða á rafrænan hátt, birtar á filmu eða látnar í ljós í mæltu máli. Á hvaða formi sem upplýsingarnar eru, og hvaða leiðir sem notaðar eru til þess að samnýta þær eða geyma, ætti ávallt að vernda þær á viðeigandi hátt.

Upplýsingaöryggi felst í verndun upplýsinga fyrir margs konar ógnum til þess að tryggja rekstrarsamfellu, lágmarka rekstraráhættu og hámarka arðsemi fjárfestinga og viðskiptatækifæra.

Upplýsingaöryggi næst með því að innleiða viðeigandi stýringar, þ. á m. stefnu, ferli, verklagsreglur, skipurit og hugbúnaðar- og vélbúnaðaraðgerðir. Þessum stýringum þarf að koma upp, innleiða þær, vakta, rýna og bæta eftir þörfum til þess að tryggja að öryggis- og rekstrarmarkmið fyrirtækisins séu uppfyllt. Þetta ætti að gera í tengslum við önnur rekstrarfræðileg ferli.

0.2 Af hverju þörf er á upplýsingaöryggi?

Upplýsingar ásamt stuðningsferlum, kerfum og netum eru mikilvægar rekstrarlegar eignir. Skilgreining, öflun, viðhald og umbætur á upplýsingaöryggi geta verið nauðsynleg atriði til þess að viðhalda samkeppnishæfni, fjárstreymi, arðsemi, hlítinu við lög og ímynd í viðskiptum.

Að fyrirtækjum og upplýsingakerfum þeirra og netum steðja ógnir úr ýmsum áttum, svo sem af svikum með aðstoð tölva, njósnum, spellvirkjum, skemmdarverkum, eldsvoðum og flóðum. Skaðvaldar, svo sem spillikóti, tölvuhakk og atlögur að þjónustumiðlun, verða sífellt algengari, ágengari og háþróaðri.

Upplýsingaöryggi er mikilvægt bæði á sviði opinbers reksturs og einkareksturs, og til að vernda mikilvæga innviði. Á báðum þessum sviðum mun upplýsingaöryggi

0 Introduction

0.1 What is information security?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

0.2 Why information security is needed?

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will

verða til auðveldunar, t.d. við að að koma á rafrænni stjórnsýslu eða rafrænum viðskiptum, og til þess að komast hjá eða draga úr áhættu sem þeim fylgir.

Samtenging almenningsneta og einkaneta og samnýting á upplýsingaaudlindum eykur vandann við að stýra aðgangi. Þróunin í átt að dreifðri gagnavinnslu hefur einnig grafið undan skilvirkni miðlægrar stýringar í umsjá sérfræðinga.

Mörg upplýsingakerfi hafa ekki verið hönnuð til þess að vera örugg. Það öryggi sem hægt er að ná fram með tæknilegum aðferðum eingöngu er takmarkað og verður að styðja við það með viðeigandi stjórnun og verklagsreglum. Til þess að skera úr um hvaða stýringar ættu að vera til staðar þarf vandlega skipulagningu þar sem smáatriðum er gefinn gaumur. Stjórnun upplýsingaöryggis krefst að lágmarki þátttöku allra starfsmanna fyrirtækisins. Hún kann jafnframt að krefjast þátttöku hluthafa, birgja, þriðju aðila, viðskiptavina eða annarra ytri aðila. Einnig getur verið þörf á ráðgjöf sérfræðinga annarra fyrirtækja.

0.3 Hvernig koma á upp öryggiskröfum

Nauðsynlegt er að fyrirtæki beri kennsl á öryggiskröfur sínar. Flokka má öryggiskröfur í þrjá megin flokka eftir uppruna:

1. Í fyrsti flokknum eru kröfur sem eiga rætur að rekja til mats á áhættu fyrirtækisins með tilliti til markmiða þess og heildaráætlunar um rekstur. Með áhættumati eru greindar þær ógnir sem stöðja að eignum og metnar veilur og líkindi á því að eitthvað komi fyrir og hver áhrifin kunni að verða.
2. Í öðrum flokki eru lagalegar, reglugerðarlegar og samningslegar kröfur sem fyrirtæki, viðskiptaaðilar þess, verktakar og þjónustuveitendur þurfa að uppfylla sem og félags- og menningarumhverfi þeirra.
3. Í þriðja flokknum eru sértækar meginreglur, markmið og rekstrarkröfur um upplýsingavinnslu sem fyrirtæki hefur mótað til þess að styðja við starfsemi sína.

0.4 Að meta öryggisáhættu

Borin eru kennsl á öryggiskröfur með skipulegu mati á öryggisáhættu. Kostnað af stýringum þarf að meta í ljósi þess rekstrarlega skaða sem líklegt er að hljótist af ef öryggi brestur.

Niðurstöður áhættumatsins koma að gagni bæði við leiðsögn og ákvörðun viðeigandi aðgerða og forgangsröð í stjórnun áhættu vegna upplýsingaöryggis og við að innleiða stýringar til verndar gegn þeirri áhættu.

function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks.

The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.

0.3 How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements.

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.
2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.
3. A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations.

0.4 Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.