Verklaring van toepasselijkheid

Referentie document en versie: SOA-UNI-NL versie 19/04/2022 Classificatie: publiek

Dit document omvat de Verklaring van Toepasselijkheid ten behoeve van de certificering voor de ISO 27001:2013 standaard. De doelstelling van dit document is het identificeren van de toepasselijke beheersmaatregelen welke geïmplementeerd dienen te zijn om de bedreigingen tegen Flowsparks Nederland BV en haar bedrijfsprocessen te controleren en te managen.

De ontwikkeling, onderhoud, beheer en support van een digitale leeromgeving en de verwerking van de daarin aanwezige persoonsgegevens.

Het management van Flowsparks Nederland BV verklaart:

- Alle controls hieronder benoemd zijn “in scope” en volgen uit de informatiebeveiligings risico-analyse als maatregel voor de behandeling van een of meer daar genoemde risico’s.
- Alle controls hieronder niet benoemd zijn uitgesloten omdat zij niet aangemerkt worden als maatregel voor de behandeling van een of meerdere risicos geïdentificeerd in de informatiebeveiligings risico analyse, en het management accepteert de restrisico’s.

privacy & security officer

www.flowsparks.com

```
LR = legal requirement
CO = contractual obligation
BP = business / best practice
RA = risk assessment
```

A5 Information security policies

5.1 Management direction for information security

nr	control	in scope	implemented	reason
5.1.1	Policies for information security	yes	yes	BP
5.1.2	Review of the policies for information security	yes	yes	BP

A6 Organization of information security

6.1 Internal organization

nr	control	in scope	implemented	reason
6.1.1	Information security roles and responsibilities	yes	yes	BP
6.1.3	Contact with authorities	yes	yes	LR
6.1.4	Contact with special interest groups	yes	yes	BP
6.1.5	Information security in project management	yes	yes	CO,BP

6.2 Mobile devices and teleworking

nr	control	in scope	implemented	reason
6.2.1	Mobile device policy	yes	yes	LR,CO,BP,RA
6.2.2	Teleworking	yes	yes	CO,BP,RA

www.flowsparks.com

A7 human resource security

7.1 Prior to employment

nr	control	in scope	implemented	reason
7.1.1	Screening	yes	yes	CO,BP
7.1.2	Terms and conditions of employment	yes	yes	CO,RA

7.2 During employment

nr	control	in scope	implemented	reason
7.2.1	Management responsibilities	yes	yes	CO,BP
7.2.2	Information security awareness, education and training	yes	yes	CO,BP,RA
7.2.3	Disciplinary process	yes	yes	CO

7.3 Termination and change of employment

nr	control	in scope	implemented	reason
7.3.1	Termination and change of employment responsibilities	yes	yes	CO,BP

www.flowsparks.com

A8 Asset management

8.1 Responsibility for assets

nr	control	in scope	implemented	reason
8.1.1	Inventory of assets	yes	yes	BP
8.1.2	Ownership of asssets	yes	yes	BP
8.1.3	Acceptable use of assets	yes	yes	BP,RA
8.1.4	Return of assets	yes	yes	CO,BP

8.2 Information classification

nr	control	in scope	implemented	reason
8.2.1	Classification of information	yes	yes	CO,BP, RA
8.2.3	Handling of assets	yes	yes	BP,RA

8.3 Media handling

nr	control	in scope	implemented	reason
8.3.1	Management of removable media	yes	yes	CO,BP
8.3.2	Disposal of media	yes	yes	CO,BP

www.flowsparks.com

A9 Access control

9.1 Business requirements of access control

nr	control	in scope	implemented	reason
9.1.1	Access control policy	yes	yes	CO,BP,RA
9.1.2	Access to networks and services	yes	yes	CO,BP,RA

9.2 User access management

nr	control	in scope	implemented	reason
9.2.1	User (de)registration	yes	yes	CO,BP
9.2.2	User access provisioning	yes	yes	CO,BP
9.2.3	Management of privileged rights	yes	yes	BP
9.2.4	Management of secret authentication information	yes	yes	BP
9.2.5	Review of user access rights	yes	yes	CO,BP,RA
9.2.6	Removal / adjustment of access rights	yes	yes	CO,BP,RA

9.3 User responsibilities

nr	control	in scope	implemented	reason
9.3.1	Use of secret authentication information	yes	yes	BP

9.4 System and application access control

nr	control	in scope	implemented	reason
9.4.1	Information access restriction	yes	yes	BP
9.4.2	Secure login procedures	yes	yes	CO,BP
9.4.3	Password management system	yes	yes	BP,RA
9.4.4	Use of privileged utility programs	yes	yes	BP
9.4.5	Access control to source code	yes	yes	BP,RA

www.flowsparks.com

A10 Cryptography

10.1 Cryptographic controls

nr	control	in scope	implemented	reason
10.1.1	Policies on the use of cryptography	yes	yes	BP
10.1.2	Key management	yes	yes	BP

A11 Physical and environmental security

11.1 Secure areas

nr	control	in scope	implemented	reason
11.1.1	Physical security perimeter	yes	yes	BP
11.1.2	Physical entry controls	yes	yes	CO,BP
11.1.4	Protecting against external and environmental threats	yes	yes	BP

11.2 Equipment

nr	control	in scope	implemented	reason
11.2.2	Supporting utilities	yes	yes	BP
11.2.3	Cabling security	yes	yes	BP
11.2.4	Equipment maintenance	yes	yes	BP
11.2.5	Removal of assets	yes	yes	BP
11.2.7	Secure disposal or re-use of equipment	yes	yes	CO,BP
11.2.9	Clear desk and clear screen policy	yes	yes	BP,RA

www.flowsparks.com

A12 Operations security

12.1 Operational procedures and responsibilities

nr	control	in scope	implemented	reason
12.1.1	Documented operations procedures	yes	yes	BP,RA
12.1.2	Change management	yes	yes	BP
12.1.3	Capacity management	yes	yes	BP,RA
12.1.4	Separation of dev, test and production environments	yes	yes	CO,BP

12.2 Protection from malware

nr	control	in scope	implemented	reason
12.2.1	Controls against malware	yes	yes	CO,BP,RA

12.3 Backup

nr	control	in scope	implemented	reason
12.3.1	Information backup	yes	yes	CO,BP,RA

12.4 Operational procedures and responsibilities

nr	control	in scope	implemented	reason
12.4.1	Event logging	yes	yes	CO,BP
12.4.2	Protection of log information	yes	yes	BP
12.4.4	Clock synchronization	yes	yes	BP

12.5 Control of operational software

nr	control	in scope	implemented	reason
12.5.1	Installation of software on operational systems	yes	yes	BP

12.6 Technical vulnerability management

www.flowsparks.com

nr	control	in scope	implemented	reason
12.6.1	Management of technical vulnerabilities	yes	yes	CO,BP
12.6.2	Restrictions on software installation	yes	yes	

12.7 Information system audit considerations

nr	control	in scope	implemented	reason
12.7.1	Information system audit controls	yes	yes	CO,BP

13 Communications security

13.1 Network security management

nr	control	in scope	implemented	reason
13.1.1	Network controls	yes	yes	BP
13.1.3	Segregration in networks	yes	yes	BP, RA

13.2 Information transfer

nr	control	in scope	implemented	reason
13.2.1	Information transfer policies and procedures	yes	yes	CO,BP
13.2.2	Agreements on information transfer	yes	yes	CO,BP
13.2.3	Electronic messaging	yes	yes	BP
13.2.4	Confidentiality or non-disclosure agreements	yes	yes	CO,BP, RA

www.flowsparks.com

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

nr	control	in scope	implemented	reason
14.1.1	Security requirements analysis and specifications	yes	yes	BP
14.1.2	Securing application services on public networks	yes	yes	BP

14.2 Security in development and support processses

nr	control	in scope	implemented	reason
14.2.1	Secure development policy	yes	yes	BP
14.2.2	System change control procedures	yes	yes	BP
14.2.3	Technical review of applications after operating platform changes	yes	yes	BP
14.2.4	Restrictions on changes to software packages	yes	yes	BP
14.2.5	Secure system engineering principles	yes	yes	BP
14.2.6	Secure development environment	yes	yes	BP
14.2.8	System security testing	yes	yes	BP
14.2.9	System acceptance testing	yes	yes	BP

14.3 Test data

nr	control	in scope	implemented	reason
14.3.1	Protection of test data	yes	yes	CO,BP

www.flowsparks.com

15 Supplier relationships

15.1 Information security in supplier relationships

nr	control	in scope	implemented	reason
15.1.1	Information security policy for supplier relationships	yes	yes	CO,BP
15.1.2	Addressing security within supplier agreements	yes	yes	CO,BP
15.1.3	Information and communication technology supply chain	yes	yes	CO,BP

15.2 Supplier service delivery management

nr	control	in scope	implemented	reason
15.2.1	Monitoring and review of supplier services	yes	yes	CO,BP
15.2.2	Managing changes to supplier services	yes	yes	CO,BP

16 Information security incident management

16.1 Management of information security incidents and improvements

nr	control	in scope	implemented	reason
16.1.1	Responsibilities and procedures	yes	yes	BP
16.1.2	Reporting information security events	yes	yes	BP
16.1.3	Reporting information security weaknesses	yes	yes	BP
16.1.4	Assessment of and decision on information security events	yes	yes	BP
16.1.5	Response to information security incidents	yes	yes	BP
16.1.6	Learning from information security incidents	yes	yes	BP
16.1.7	Collection of evidence	yes	yes	BP

www.flowsparks.com

17 Information security aspects of business continuity management

17.1 Information security continuity

nr	control	in scope	implemented	reason
17.1.1	Planning information security continuity	yes	yes	BP
17.1.2	Implementing information security continuity	yes	yes	BP
17.1.3	Verify, review and evaluate information security continuity	yes	yes	BP

17.2 Redundancies

nr	control	in scope	implemented	reason
17.2.1	Availability of information processing facilities	yes	yes	BP

18 Compliance

18.1 Compliance with legal and contractual requirements

nr	control	in scope	implemented	reason
18.1.1	Identification of applicable legislation and contractual requirements	yes	yes	BP
18.1.2	Intellectual property rights	yes	yes	LR
18.1.3	Protection of records	yes	yes	LR,CO,BP
18.1.4	Privacy and protection of personally identifiable information	yes	yes	LR,CO,BP

18.2 Information security reviews

nr	control	in scope	implemented	reason
18.2.1	Independent review of information security	yes	yes	CO
18.2.2	Compliance with security policies and standards	yes	yes	BP
18.2.3	Technical compliance review	yes	yes	CO,BP

www.flowsparks.com

Flowsparks custom controls

nr	control	in scope	implemented	reason
FS-01	Appropriate User instruction for customers	yes	yes	RA
A5.7	Threat intelligence	yes	yes	BP
A8.10	Information deletion	yes	yes	CO, BP

www.flowsparks.com