Guide to companies about the safety of personal data

Introduction

A good risk analysis allows us to determine to what precautions needs to intervene to ensure the safety of the data.

Persónuverndarlöggjöfin specifies that the protection of personal data will be required to take appropriate technical and skipulagslegra measures in accordance with the risks.

Such an approach allows businesses and organizations to take objective decisions and make changes in accordance with the situation. However, it is often difficult for the person who is not such to make arrangements with the qualifications and make sure that appropriate arrangements have been made.

These instructions describe them lágmarksráðstöfunum which businesses and organizations need to do to meet the legal requirements. Note that the instructions are of a general nature and is required to take account of the nature and scope of the processing of personal data when safeguards are certain. Thus, are not made the same requirements to a company that wins a small amount of general personal data such as the name, address and telephone number and, for example, the healthcare facility who works large quantity health information. Those are the instructions first and foremost intended for small and medium-sized entities but those who work with an extensive amount of personal and/or sensitive personal information may need to seek external expert assistance or even earn a certification. Then take the instructions not to specific safety measures that may need to be done in certain sectors, such as in the financial market or in the healthcare sector.

In summary, one can describe the process of setting up a system of information security, in the following way:

Registry upplýsingaeigna

- The hardware used for the registration and storage of the personal data area
- Software
- Connection technology (Internet, fiber optic cable, innanhúsnet, wifi)
- The documents on the paper

Registry effects

- Óleyfilegur access to the data
- Unauthorised change of data
- Unexpected barrier of access to data

The registry risks

- Access óleyfilegra internal users
-

- Access the system administrator
- Access external aggressor
- Access of competitors
- Damage other than of man-made (fire, water, etc.)

Analysis of potential risk factors

- The data used in an inappropriate way
- Tölvuóværu occur, viruses, lyklaborðshlerun
- Data lost
- The data come surprise for the eyes unauthorized party
- Data damaged due to an accident or skemmdarverks
- The data difficult to access because of the space, netstíflu

Analysis of means

- Permissions
- Copying
- Traceability of access, action
- Öryggisúrræði housing
- Encryption
- Information made non-identifiable

Analysis áhættustigs

- Insignificant
- Slight
- Significant
- High

The tablet of this type can be used to assess the formal relationship of risk factors:

Risks
Impact on
individuals
The main
áhættuvaldar
Main risks
The current or
projected
response
Severity
Probability
Unwanted

access to
data
Unwanted
modification of
the data
Data will be lost

Here is an example of such a áhættutöflu for any particular processing persónuuppýsinga. Note however that in certain cases you may need to use other frequencies are defined as, e.g., the case of particularly sensitive personal information is involved.

Probability/Impact

Low impact - 1

Medium impact - 2

High impact - 3

Very high impact - 4

Rarely – 1

(less than annual)

1
2
3
4

Fairly often – 2

(<monthly)

2
4
6
8

Often – 3

(<weekly)

3
6
9
12

Very often – 4

(<daily)

4
8
12
16

In this case, there are different reactions after the product of the likelihood and risk.

Green (1-2) – No specific response required, risk analysis acceptable.

Yellow (3-6) - better View, check whether the response is needed, better security, memory collection, etc.

Red (7+) – Processing assessed as too risky, there is a need for increased security or memory processing.

Installation and testing

If the resources that are present or deciding to put out of place are assessed relevant the need to walk from sure that they are tested and used where appropriate.

Follow-up

After the resources are set up is required to install the control system where the rules are followed and walked out of
the shade of the resources is followed in a systematic way.

An overview of what needs to be done to ensure the safety of the

1. Add öryggisvitund users
2. Authentication of users
3. Permissions
4. Atburðaskráning and atvikastjórnun
5. Security vinnustöðva
6. The safety of remotely
7. The protection of the internal network
8. Security servers
9. The security of the sites
10. Data security
11. Secure langtímageymsla
12. Gagnaviðhald and support
13. Monitoring with vinnsluaðilum
14. Security gagnasamskipta
15. Physical security
16. Monitoring with software development
17. Encryption, electronic signatures, integrity

1 – Add öryggisvitund users

Each user needs to be aware of privacy and security risks of a business or organization

Grunnúrræði

 Increased öryggisvitund users with educational, alerts, training courses, etc.

 Document processes and make sure that the documentation is kept with the

 Write procedures for the handling of data and information system, e.g.

○ let the it department know about all violations of safety rules, attempts to break, etc.

○ never let third parties get the password or aðgangsauðkenni

○ do not set up, copy, edit, or delete the software without a license

○ lock the workstation when it is not in use

○

do not view, try to view or to remove the data which is not related to the tasks the user

○

follow the rules of the company about the treatment of storage devices are and get a license for all gagnaafritun

○

follow the rules on the use of mobile, einkageymslusvæða, their own devices, Internet and telephone

○

familiarize themselves with how the registration of the events and aðgangshindrunum package

○

familiarize themselves with what consequences may result from violations of the rules

Additional resources

▯

Put up gagnaflokkunarkerfi with a few aðgangsstigum

Tick particularly sensitive data

Held regular workshops and meetings about information security to increase awareness

See to it that users sign a privacy statement or discussion of confidentiality in employment contracts. If employees fall under the statutory confidentiality, e.g. the government, financial institutions and other parties the right to take it out

2 – Identification of users

To the fact that users use only the data they are supposed to have access to , the need to identify that they are they who they claim to be before they receive access to personal information

Ids can be classified into three:

- Something the user knows (e.g. password)
- Something that the user is using (e.g. auðkenniskort or electronic identification on a phone)
- Something the user is or does (e.g. a fingerprint or signature)

Strong authentication uses something half of this hat-trick.

Grunnúrræði

- Enjoy the identifier for each user and the ban to more users samnýti it. If this is unavoidable, it should get the permission of the management and set up a system to record the use of
- Follow the rules of the team for the safe placement of password length, expiration date, and complexity (use a certain minimum number of digit and tákngerða)
- Grab some actions can a user do not enter the correct password in a certain number of experiments, e.g. to block an account temporarily or permanently, or offer the Captcha-solution
- Let the user change the password when he identifies himself to the system for the first time

It needed to avoid

- Let the other have his password or other identification
- Write down the password in the ódulkóðaða file, on paper or anywhere else where others can possibly get it
- To save the password in the browser without the use of yfirlykilorð
- To use the password that testifies in the personal data such as the name, date of birth, etc.
- To use the same password on more than one place
- To use the default password continue
- Send password via e-mail

Additional resources

- Enjoy lykilorðageymsluforrit (e. password manager) to keep track of passwords in different places and use only one yfirlykilorð
- Enjoy the strong (double-stranded) authentication where possible
- Let fewer attempts for authentication and finished to the user if they become too many
- Requires that passwords are regularly updated
- Let the users do not use the default usernames or passwords producers

□

Save the password encrypted (all operating systems, databases and browsers do this)

3 – Access

The permit only to access to the documents that use ndinn really need access to

Grunnúrræði

□

I want to know access depending on the needs and role so that users have only access to the data they need, their work due to the

□

Finished on the access of users when they retire

Slip the annual passage of the access of the user to ensure that not are substitutes notendareikningar and you can hone in on the needs for access

It needed to avoid

To create or use a common user accounts

To give kerfisstjóraaðgang those who do not have a need for him

To give users more access than they have a need for

Forgetting to withdraw heightened access permissions that are supposed to be temporary (e.g. due to forfalla)

Forget to invalidate the access of users who have stopped or moved to in the work

Additional resources

Put up aðgangsstýringarstefnu in accordance with the processes of the institution or company. It shall specify:

○

What should be done when the users start and stop

○

The consequences of the fact that do not follow the safety rules

○

Any leads are allowed to restrict and control access to personal information

4 – Atburðaskráning and atvikastjórnun

In order to be able to be aware of and respond to unlawful access to personal data, the unlawful use of them, and trace the origins of the incidents need to register the event in the computer systems and have a formal process to respond to incidents

Grunnúrræði

Put up the log files (log off now) as file access and user authentication, anomaly and security incident with the timing of the

Put up a detailed registration of all the actions of users where sensitive information is involved

Teach the users if such atburðaskráning is present in accordance with the requirements of persónuverndarlaga

Ensure that the access is directed to skráningarvélbúnaði and software so that those users who need to register does not come in the documentation

Record the data processing and scrutinized such registration periodically to ensure that it is in the normal process

Ensure that those who manage the registration notify you of abnormal incidents and violations

Inform to the protection of Privacy if a security breach must be due to access to personal information

Inform to the persons involved, in plain and simple terms if the security breach will be due ólögmæts access to personal information if it comes with a high risk for the rights and freedoms of their

It needed to avoid

- To use the log files to another but they are intended, e.g. it is forbidden to use them to monitor the presence of users in the work

5 – Safety vinnustöðva

The dangers of tölvuinnbrotum are significant and vinnust öðvar are often aðgangspunkturinn

Grunnúrræði

- Adjust the workstations so that they will lock automatically if they have been unused for a certain period of time
- Put up a firewall so that the closed is unused port
- Uppfærið operating system, vírusvarnir and other software regularly
- Adjust the operating system and software so that he'll update itself automatically, if possible
- Save the user data on a central, afrituðum disksvæðum rather than on the vinnustöðvunum yourself
- Limit the use of media (e.g., drifter, minnislykla) to it of all the essentials
- Turn off the automatic execution of media (e. autorun)
- Ensure that the user knows or will receive a notification if the be is to apply to the workstation outside from

It needed to avoid

- Using outdated types of operating systems
- To give users the stjórnaðgang (e. admin rights) if they may not want him to go

Additional resources

- Avoid the use of external applications that do not come from trusted sources
- Avoid using applications that require stjórnaðgangs
- Delete the data of the workstation if she goes to another user
- Price of the security incident on the workstation needs to investigate how it happened and whether it has reached to other parts of the decoration and so
- Carry out regular here you can change and control
- Uppfærið software uppgötvist öryggisgallar in him
- Uppfærið operating system regularly and automatically

6 – Security to remotely

Do assume that a mobile device can be lost or stolen and make the arrow yggisráðstafanir with that in mind

Grunnúrræði

- Increase the awareness of users about the dangers of using mobile devices (laptops, mobile phones) and make measures to reduce these risks
- Put up a replication - or samstillingarkerfi for mobile devices in order to protect against loss of data
- Set up encryption for mobile devices, and loose data sources, the whole disk if it is possible, otherwise the single files or data storage
- Requires that the mobile is locked with a auðkennisnúmeri, pattern or such
- If using with the service he needs to lay out adequate insurance for the fact that he can carry out security measures

It needed to avoid

- To use the out of hand built skýjalausnir without carefully check their terms and safety regulations

Additional resources

- Enjoy skjásíu on laptops that are used in public places (so not visible on the screen from the side)
- Limit the data that are stored on the mobile devices to what is strictly necessary
- Do measures against theft (öryggiskapall, visible markings) and to minimize the effect of his (automatic locking, encryption)

Dulkóðið connection and the data and lock the device after use when mobile devices are used to collect data on the visit (through a web browser, email)

7 – Protection of the internal network

The license only those network connections as needed

Grunnúrræði

▯

Limit Access by closing for unnecessary services

▯

Dulkóðið all wireless networks and slip on those complex passwords. Networks that are open to visitors shall be separated from internal networks

▯

Requires that the VPN is used for remote connections into the internal network, preferably with a strong (double-stranded)
identification

▯

Ensure that the control panel of the software or services are not accessible directly from the Internet

It needed to avoid

□

To use ódulkóðaðar connections on the board to *telnet* to connect to the netbúnaði. Enjoy secure connections like *ssh* (e. Secure Socket Shell) or direct access with a cable

□

To set up a wireless network with WEP encryption. Always use WPA2 or newer encryption

Additional resources

□

Various european institutions in the field of data protection and information security (ICO, ENISA, ANSSI) have issued instructions (in English) about the security of sites, samskiptastaðalsins TLS (e. Transport Layer Security) and wireless networks, which can introduce a

□

It is possible to carry electronic identification on the device and prevent unknown devices from connecting to the internet

Árásargreining (e. Intrusion Detection System) can detect the network traffic and stop possible
attacks on the equipment. It needs to inform the users about it if their traffic is analyzed under the
persónuverndarlöggjöfinni

Niðurskipt networks can reduce the influence of the individual parts will be for the intervention.
Separate should the external network (DMZ De-Militarized Zone) where web servers, mail servers, etc.h. are housed,
from the intranet

8 – Security servers

To ensure the security of the servers is for all w r as they host a lot of data

Grunnúrræði

Given only qualified people stjórnaðgang and access to stjórnborðum and instru

Enjoy the user with the memory access for other jobs

Have password rules for stjórnnotendur and change the password when any of their stops

Insert into security updates without delay when they are received

Enjoy sérgagnagrunnsnotanda for every application

Take regular backups and test them regularly

Set up TLS encryption and authentication for all web services

It needed to avoid

To use its precarious services (ódulkóðuð highlighting, ódulkóðaður gagnastraumur)

To put the databases on machines that also host other services (tissues, mail, chat)

Let the databases to be accessible directly from the internet

To multiple access (users that are used by more than one person's or service)

Additional resources

Separate multiple systems that work sensitive information from other systems

In larger networks should administering to take place from the separate stjórnneti which is secured with strong authentication and atburðaskráningu

Look and inspect the vulnerable system with netgreiningartólum such as nmap (e. Network Mapper) to
detect the possible öryggisholur. Insert a system to limit the auðkenningartilraunir

Limit access to stjórnportum and stjórnborðum software and firmware

9 – the Security of the sites

All sites need to identify themselves and the correctness of the data they disseminate or collect the

Grunnúrræði

Set up TLS encryption

- Skyldið TLS on all pages that collect or display data that does not have to be open to the public
- Completed for traffic on all ports that are not needed on
- Given only qualified people stjórnaðgang and limit the use of stjórnnotenda with such
- Get the consent of the user if you are to collect the cookies which are not strictly necessary for the functionality of the website
- Do web solutions't more complicated than it needs to be, remove the unused subsystem and uppfærið then the parts which are used

It needed to avoid

- Putting personal data on board we usernames or passwords in urls (URL)
- To use ódulkóðaðar services and authentication
- To use the servers as workstations, especially not use them to browse, download mail or chat
- To install the databases on a serving that are directly accessible from the Internet
- To let many people share the same user (e.g., administrator, root)

Additional resources

- Consult the lawful and proper use of communications and other such tracking the use of
- Scan servers regularly with regard to safety and service
- Familiarise yourself with the rules of the ICO, ENISA, ANSSI
about the installation of TLS encryption on the servers

10 – data Security

Copy the required data and test copies regularly. Make the required plan of action to ensure business continuity if to gagnat aps or vélbúnaðarbilunar comes

Grunnúrræði

- Set up regular backup. Preferably daily síhlutaafritun (e. progressive incremental backup) and the full backing occasionally, e.g. in three months
- Store the copies outside the company or organization, preferably in a fire - and vatnsvörðu space
- Protect the duplicates as well as netþjónana itself, with encryption and access control list
- Dulkóðið afritunarstrauminn if he goes over the network
- Make an action plan about how to respond to loss of data or other shocks
- Ensure that users, hýsingaraðilar and subcontractors know who to contact when
incidents become
- Test the backup and recovery of their on a regular basis to ensure that they are right and the right

Use the battery (UPS) to protect the equipments for power outages

Ensure that the data are stored on multiple disks (RAID) for safety

It needed to avoid

Do not store a copy in the same place and the machines that host the frumgögnin. Fire - or water damages could e.g.
caused to either of the two was lost in one of the

Additional resources

Consider to make an action plan for response to major possible shocks. Guidelines for
such can be found widely on the internet

If the data are very important may be considering to bring up the double netþjónakerfi at each site

11 – Safe langtímageymsla

Data that are not longer used regularly but that could've be necessary in the future, e.g., for legal reasons, sometimes you have to save in the langtímaskjalasafni

Grunnúrræði

- Identify the needs of the skjalasafnsins, what should be stored? Where? How long?
- Identify the aðgangsþarfir skjalasafnsins
- When it comes to deleting data permanently, make sure that they've really been destroyed completely

It needed to avoid

- To use geymslugögn with ónógan the life cycle, e.g. it is not possible to trust that the data are accessible on the skrifanlegum CD and DVD drives longer than 4-5 years
- To store the older data in the database which is in full use
- Store pappírsgögn in plastmöppum or with bréfaklemmum/staples

Additional resources

- In the law on official archives are afhendingarskyldir parties to Þjóðskjalasafns/héraðsskjalasafna defined, e.g. the ministry, the courts, agencies and local authorities, etc. the Sources of these entities to delete information are very limited. The bears at the same time to act recordkeeping in accordance with the rules of the Þjóðskjalasafns (https://skjalasafn.is/reglur_og_leidbeiningar)
  - Among other things, the need to make sure that the folders are sýrufríar and that the data are not stored in the plastmöppum or the content of the paper clips, as this can empty the data that should go in the langtímavarðveislu

12 – Gagnaviðhald and support

Data storage need to organize to control the access to them. The data needs to spend before the hardware is deleted or sold

Grunnúrræði

- Held centrally track of how gagnamiðlar are copied, moved or deleted
- Insert a clause about the information security in the viðhaldssamninga hosting provider and contractor
- Let the qualified staff to monitor the works of the third party
- Have clear procedures on wipe and go after them
- Delete data safely of the hardware before it is thrown away, sold, sent to repair or at the end of the rental

It needed to avoid

- To install the software for remotely which is insecure, e.g. using ódulkóðaðar data connections

Reuse, sell or throw away gagnamiðlum without delete the data of them safely

Additional resources

Use should be witnessed gagnaeyðingarhugbúnað

13 – Control vinnsluaðilum

To ensure the safe treatment of the personal data area which are processed by its subsidiary contractors or service providers

Grunnúrræði

Use only processors which can guarantee the sufficient skills, knowledge and capacity

Let the processors write under the privacy statement

Explore and document how vinnsluaðilinn intends to ensure data security, including data encryption and gagnastrauma, access control, identification and atburðaskráningu

Make a written contract we vinnsluaðilann outlining the challenges, scope, time period and purpose of the processing as well as the obligations of each party. Privacy has prepared a model to vinnslusamningi that can be used. It is important to ensure the identification, proper treatment of information (the destruction or return) to the processing of completion and reporting requirements if the deviation will be

It needed to avoid

Let the processors start the processing of personal data without a valid, written contract
to that effect

To use the cloud-based service without having information about the location of gagnageymslna or without order to ensure the legitimate data transfer outside of the EEA-area

Additional resources

See 28. gr. pvrg.

A model to vinnslusamningi

Receive a confirmation of the adequacy of insurance

14 – Safety gagnasamskipta

Ensure the safety of all the transit character of information and remember that the email system and electronic communication systems are not secure channels for communication without additional measures and to all who have access to the relevant servers might have access to your data

Grunnúrræði

Dulkóðið data to send in the storage device (USB, DVD, drifter) to a third party

Dulkóðið data to be sent over the internet using HTTPS, SFTP

Do not send the password dulkóðaðra files with your own files

If use need a fax, send only on the fax that has secured access

It needed to avoid

To send ódulkóðuð data with the private e-mail

Additional resources

If possible, put up lyklaða encryption and digital signatures with public and einkalyklum

15 – Material safety

Ensure the safety of the housing in which the gagnaþjónar and netbúnaður are hosted. Needs to be prevented for unauthorized access or inhibit him as far as possible

Grunnúrræði

Put up the alarm and ensure that the monitor

Put up smoke detectors and fire-fighting equipment and scrutinized annually

Separate the area after the tenderness, e.g. by limiting access to the tölvurými

Keep a list of those who have access to each area and held the charts the

Put apis, e.g. by letting the employee always follow external sources

Protect computer equipment with specific equipment, e.g. eldvarnarbúnaði, upphækkuðum the shelves to prevent water damage, the double electrical systems and ventilation

It needed to avoid

▯

To vanáætla size or viðhaldsþörf tölvurýma. If the system on the board with the electrical system, the batteries or the ventilation fails, can load ceased to function, data can be lost or access to the them
opens up

Additional resources

File access to areas where personal data are stored. Memorize the staff that such
registration is in progress

See to it that only the authorized personnel is allowed to enter the sensitive area and that it needs to
carry on a visible identification (authentication with the photo)

Visitors, e.g. technicians, has limited access and to come, and their departure are recorded

Go regularly over the permissions of sensitive areas and change them when necessary

16 – Control software development

Security and privacy need to be embedded in every software development from the beginning.
It is necessary that the software give users control over their information and that he
is protected for errors, loss of data, trespassing tional changes or abuse

Grunnúrræði

Build privacy and security into the design of the software from the beginning. This can affect it
any ways and solutions are selected

Ensure always that the greatest security is the default setting in the software that is intended to the public

Avoid innsláttarsvið with free text or notes if possible

Put up a separate þróunarumhverfi for the development and programming and enjoy fictional or
ópersónugreinanleg data

It needed to avoid

To use the actual data during the development or testing. Use fictional data everywhere where it
will be established with the

To develop software without taking into account security and privacy

Additional resources

Only collect them lágmarksgögnum necessary, e.g., if only the need for
year of birth should not let the program download the month and day, too

Choose should be geymsluform after the storage period as estimated is, e.g. if your intention is to store
the data in the 20 years is appropriate to choose an open gagnaform that it is more likely to be supported for a
longer
time

Access control should be embedded in the software development from the very beginning

In many cases it is advisable to ensure the code with the electronic signature to ensure to not
have been tampered with he

17 – Encryption, electronic signatures, integrity

It is important to preserve the integrity, confidentiality and integrity of data. Hakkaföll can be used to ensure the integrity of the data, the origin can be secure with electronic signatures, and the confidentiality with encryption

Grunnúrræði

- Enjoy-known and recognized algorithm (algóritma) and uppfærið depending on your needs (can change and will change)
  - SHA-256, SHA-512 or SHA-3 which hakkaföll
  - HMAC/SHA-256, bcrypt, scrypt or PBKDF2 to store passwords
  - AES or AES-CBC for symmetrical encryption
  - RSA-OAEP for asymmetric encryption
  - RSA-SSA-PSS for electronic signatures

It needed to avoid

- To use the obsolete algorithms such as DES and 3DES for encryption or MD5 or SHA1 as hakkaföll

Confused hakkafalli and encryption or to believe that hakkafallið one is sufficient to ensure privacy. Although hakkaföll are “unidirectional”, i.e. e. difficult to turn back, it is sometimes possible to reconstruct the data from the hack. Hakkaföll are designed to be efficient, and therefore, it is sometimes possible to hack every possible inngögn (e.g. password) and thus the data

Additional resources

Inspect electronic identity documents and confirm that their use is in accordance with that which is intended is, that they
are valid and that they apply staðfestingarkeðju

Enjoy the confirm software - and dulkóðunarpakka

Use approved and verified methods of encryption, e.g.

○

The GNU Privacy Guard (GPG)

○

Solutions verified by ENISA

○

VeraCrypt software

ÖRYGGISMAT FOR A BUSINESS OR ORGANIZATION

What needs to be done

Grunnúrræði

✔

1

Add öryggisvitund users

Increased öryggisvitund with education, reminders and courses
Document processes and see to it that the documentation is kept with the

2

Authentication of users

Enjoy the unique identifier for each user and do not share it
Follow the rules for safe placement, age and complexity of the password
Respond if the user can not enter the correct password
Requires that the user change the password for the first time

3

Permissions

I want to know access depending on the needs and role of the user
Finished on the access of those who retire
Take regular passage over user accounts

4

Atburðaskráning and
atvikastjórnun

Put up the log files over access, deviations and incidents
Note whether the advanced atburðaskráningar is needed
Let users know of atburðaskráningu
Ensure access to atburðaskrám
Record the data processing and abnormal incident
Inform your Privacy, and/or other authorities (e.g. the police, the FSA, the CERT-PH) öryggisbrest

5

Security vinnustöðva

Adjust the workstations so that the locks will automatically
Uppfærið operating system, vírusvarnir and other software regularly
Set up automatic updates of the operating system and software
Save notendagögn centrally
Limit the use of storage devices are
Turn off the automatic execution of storage devices are
Ensure that the user knows that if the direction is to the workstation from the outside

6

The safety of remotely

Increase the awareness of users about the dangers of using a mobile device
Set up backup for mobile devices
Set up encryption for mobile devices

Requires that the mobile is locked with the identification of

7

The protection of the internal network

Limit network traffic to the necessities

Set up encryption for wireless networks

Requires that the VPN is used for all remote connections

8

Security servers

Given only qualified people kerfisstjóraaðgang

Install security updates without delay

Take regular backups and test them

9

The security of the sites

Set up TLS encryption

Ensure that the password and usernames are not in the urls

Ensure that the notendagögn are not taken into without inspection

10

Data security

Set up a safe tar

Store the copies in a safe place

Ensure safe transport of copy

Do regular tests on copies

11

Secure langtímageymsla

Put up aðgangskerfi for langtímaafrit

Spend langtímaafritum safely when the time comes

12

Gagnaviðhald and support

Put up a registration system for gagnaviðhald and destruction

Let the qualified staff monitor the work of a third party

Delete all the data of the hardware that is deleted or sold

13

Monitoring with vinnsluaðilum

Do selectively contract with all processors

Make a contract for the destruction or return of data after processing

Delete the data of the hardware that is returned, destroyed or sold

14

Security gagnasamskipta

Dulkóðið data to send over the network

Always make sure the correct recipient

Send password and not with themselves

15

Physical security

Lock invariably the entrance to kerfisrými and limit access

Put up your alarm and test it regularly

16

Monitoring with software development

The barley information security into software from the beginning

Avoid innsláttarsvið with the free text

The exam software with skálduðum data

17

Encryption, electronic signatures, integrity

Enjoy the well-known and recognized dulkóðanir

Keep the identity and encryption keys securely