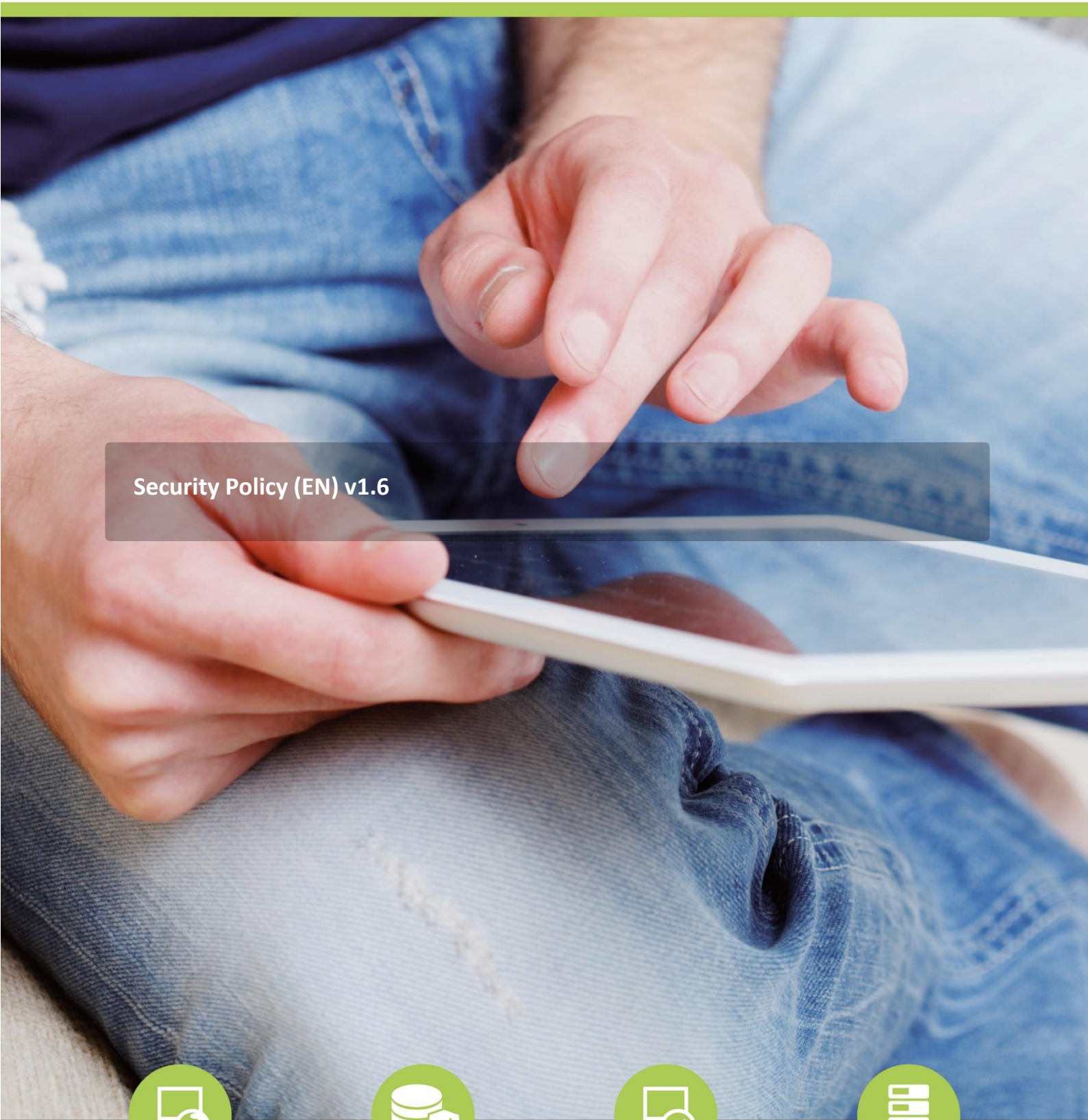
HARBERS ICT



Security Policy (EN) v1.6

Online werkplek

ICT uitwijk

Systeembeheer

Hostingdiensten

Author:	Erik Klein Langenhorst
Date:	May 25, 2018
Classificatie:	2 – Intended for stakeholders only

Version History

Version	Date	Name	Changes
1.0	*07-20-2017*	*Erik Klein Langenhorst*	*Translation of v1.2 of the Dutch Security Protocol*
1.1	*07-25-2017*	*Erik Klein Langenhorst*	*Completed translation. Minor corrections.*
1.2	*09-11-2017*	*Erik Klein Langenhorst*	*Changes and additions after ICT Recht Review*
1.3	*09-14-2017*	*Erik Klein Langenhorst*	*New layout, minor changes after Review Emiel Harbers*
1.4	*09-21-2017*	*Erik Klein Langenhorst*	*Minor corrections after errors found while translating to Dutch*
1.5	*02-19-2018*	*Erik Klein Langenhorst*	*Have clarified our endpoint protection measures and added asterisks for our standard measures.*
1.6	*05-25-2018*	*Fedde Giesen*	*Added the Sub-processors of Harbers ICT to the protocol*

Contents

Purpose and Background

This security protocol is part of the Agreement that the Customer ("Data Controller") has entered into with Harbers ICT ("Data Processor") and is meant to provide insight into the technical and organizational measures that Harbers ICT has implemented as a Data Processor. This security protocol applies to all services Harbers ICT Delivers from its data centres. The most recent version of this document can always be requested by e-mail at support@harbersict.nl. This document may also be used as a reference for Harbers ICT customers that have not entered into a Data Processing Agreement with Harbers ICT.

Under the GDPR the Data Controller is responsible for determining whether the technical and organisatorial measures are sufficient for the type of data that is processed by the Data Processor. Are you reading this in your role as a Data Controller and do you have any questions after reading this document? Harbers ICT is ready to answer your questions.

Revision Frequency

This document will be revised on a yearly basis. It will also be revised when important changes to the Harbers ICT Security Policy have been made. Harbers ICT reserves the right to revise its Security Policy one-sidedly, but only if it doesn't negatively impact the level of security.

Nature of Data Processing

Within the context of the Data Processing Agreement Harbers ICT can perform different types of data processing, such as: Hosting of websites or web applications, cloud storage of (personal) data and the hosting of applications in online workspaces. Harbers ICT will only provide the IT infrastructure in which the Data Controller can store the data. The Data Controller determines the means and purposes for the processing.

Risks

Within the context of Data Processing, the Data Controller is at risk of unauthorized data processing such as damage of data, unauthorized access, changes of the data. If it cannot be reasonably ruled out that a breach of the security measures has led to one of these unauthorized actions, according to EU law this has to be considered a data leak. These risks are described below.

Unauthorized access

An unauthorized person gaining unauthorized access to the data, e.g. by circumventing security measures or procedures.

Damage or Destruction

The Responsible Party's data is damaged or destroyed. The cause may, for example, be a virus or malware but it can also be human error.

Unavailability

In case of unavailability the data is still present but the Responsible Party is unable to access the data as a consequence of (infrastructural) problems on the Data Processor's side.

Measures

Harbers ICT shall use reasonable efforts to ensure an adequate level of security of the data it processes to prevent abuse and unauthorized use as described in the Data Processing Agreement. Harbers ICT can take the following measures to mitigate the aforementioned risks. The actual measures taken are described in the Agreement or SLA.

All standard measures are marked with an Asterisk*. We always take these measures, regardless of the Services you're purchasing.

Encryption of digital files containing personal data*

If there is a need to store digital files containing personal data on external media or to (digitally) transfer those files we will ensure that the files and connection are encrypted. We shall use a minimum of the following Encryption standards.

- Key exchange: Diffie–Hellman key exchange with minimum 2048 bits
- Message Integrity: HMAC-SHA2
- Message Hash: SHA2 256 bits
- Assymetric encryption: RSA 2048 bits
- Symmetric-key algorithm: AES 128 bits
- Password Hashing: PBKDF2, Scrypt, Bcrypt.

Logical access control, using a password and a one-time access token*

Harbers ICT online workspaces are equipped with an access control mechanism that requires the use of a password and a 2-factor authentication token. A 2-factor authentication token is a personal identification number that can be generated using an app on your cell phone or a token generation device. Other services are only secured with a password. This applies to e.g. the webmail service.

Technical measures for network security

Depending on the services you have subscribed to, we will use the following technical measures to secure your services.

- ⇨ Network Partitioning and Isolation
  - Our network design incorporates VLAN configuration to partition our servers into distinctive segments. Every Customer receives their own VLAN unless otherwise specified.
- ⇨ Check Point Next Generation Threat Prevention, consisting of:
  - Next Generation Firewall*
  - Application Control
    - The Application Control Software Blade controls access to over 5,200 applications and 240,000 social network widgets with the industry's largest application coverage. It creates granular security policies based on users or groups to identify, block or limit usage of web applications and widgets like instant messaging, social networking, video streaming, VoIP, games and more.
  - Anti-Bot

        - The Anti-Bot Software Blade detects bot-infected machines, prevents bot damages by blocking bot cyber-criminal's Command and Control center communications, and is continually updated from ThreatCloud
    - Antivirus
        - The Antivirus Software Blade stops incoming malicious files at the gateway before the user is affected with real-time virus signatures and anomaly-based protections from ThreatCloud™Identify over 4.5 million malware signatures and 300,000 malicious websites with a constantly-updated worldwide network of sensors that provide ongoing malware intelligence.
    - Identity Awareness
        - The Identity Awareness Software Blade provides granular visibility of users, groups and machines, enabling unmatched application and access control through the creation of accurate, identity-based policies.
    - Anti-Spam and Email security*
        - The Check Point Anti-Spam & Email Security Software Blade provides comprehensive protection for our messaging infrastructure. A multidimensional approach protects our email infrastructure, provides highly accurate anti-spam coverage and defends organizations from a wide variety of virus and malware threats delivered within email.
    - Intrusion Prevention System
        - IPS provides a complete Intrusion Prevention System security solution, providing comprehensive network protection against malicious and unwanted network traffic, including:
            - Malware attacks
            - Dos and DDoS attacks
            - Application and server vulnerabilities
            - Insider threats
            - Unwanted
    - URL Filtering
        - The URL Filtering Software Blade controls access to millions of web sites by category, users, groups and machines with cloud-based technology that is constantly updated with new websites to support employee productivity and security policies.

Antivirus software*

We install state of the art antivirus software on our own servers as well as on customer servers/VPS'es.

Spam Filtering*

To secure our e-mail platform we use a Barracuda Email Security Gateway. This is an email security gateway that manages and filters all inbound and outbound email traffic to protect your organization from email-borne threats and data leaks.

Backups*

We use specialised backup software to back up your data. We host our own backup infrastructure in a second Equinix data centre (location Zwolle). We have a private connection between these data centers. Retention times vary per product and are specified in your service agreement or SLA. We offer granular restore options to be able to restore separate files, e-mail items, AD items or an entire VPS.

VPN*

We use a multi-layered network setup with a separate management network. We use Check Point Endpoint Remote Access VPN software to securely connect to our management network.

DDoS Protection

Distributed Denial of Service attacks are increasingly common and can cause network outages in unprotected infrastructures. We offer Equinix AntiDDoS defense as an optional service against DDoS attacks. For more information see: http://www.equinix.nl/services/managed-services/security-performance/anti-ddos/

Secure connections*

All connections to our sites, portals and support desk are secured using TLS. We also offer the possibility to set up TLS connections to the websites we host for our customers (at an extra charge). Where this is possible we only use Strong Ciphersuites and protocols.

Server Hardening

Where applicable we follow guidelines set up by the Center for Internet Security for server hardening for Microsoft Windows Server. For more information visit https://www.cisecurity.org/cis-benchmarks/.

Secured internal network*

Organisational and physical measures also apply to our internal network. Our employees cannot access the internal server space without permission. Our internal network has been secured using firewalls, virus scanning and spam filtering.

Endpoint protection*

Of course, we have secured our office network using a Next-generation Firewall. All of our computers have a antivirus software and our mail is filtered by the Barracuda spam filtering that we also use for our customers. We use bitlocker encryption and our Mac computers use Filevault encryption.

Organisational measures for access restrictions*

Only employees who need access to perform their work have access to personal data. They have signed an NDA (Non-Disclosure Agreement) with a penalty clause. You can also sign a Non-Disclosure Agreement with Harbers ICT to contractually record that Harbers ICT will not use the possibility to access the data for other reasons than to perform necessary processing.

We provide regular training to Employees to help them understand the value of protecting Customer and Colleague information and their role in keeping this data secure.

We have procedures in place to ensure our employee’s access rights are correctly altered or revoked in case of changes in or termination of employment.

Physical access control*

The hosting services that Harbers ICT provides are delivered from a high security Equinix data center. Access to facilities and equipment is restricted to a limited number of employees, and only after an identity check. External suppliers are only allowed access under direct Employee supervision. The data center is under permanent video surveillance.

Random audits

Harbers ICT will randomly audit whether access restrictions are set up correctly and whether policies are being followed correctly. Furthermore, Harbers ICT is working on implementing a security policy based on ISO 27001 guidelines. Part of this implementation process is the performance of regular third party audits.

Sub-processors of Harbers ICT

The Sub-processors of Harbers ICT are listed in the table below. Based on the service you purchase from Harbers ICT, Harbers ICT may use one or more of these Sub-processors to provide the service to you.

Name Sub-processor	**Service**	**Product**	**Purpose of transfer**
Check Point Software Technologies	Security	Check Point Firewall	Activation Check Point Firewall
Cisco Meraki	Managed Wifi	Meraki	Offering service and support
Cisco Systems, Inc.	Managed Wifi	Cisco	Offering service and support
Citrix Systems, Inc.	Online workspaces	Citrix	Offering service and support
Dell Inc.	Hardware delivery	-	If supplier requires data for delivery of the order
DigiCert Inc.	Security	SSL certificate	Perform the service
ESET	Antivirus	ESET Endpoint Security	Request license / offering service and support
Ingram Micro	Hard-/software delivery	-	If supplier requires data for delivery of the order
Mail Chimp	-	-	Perform the service
Microsoft Corporation	Office 365	Office 365	Offering service and support
Tech Data	Hard-/software delivery	ESET Endpoint Security	If supplier requires data for delivery of the order
TransIP	Domain name registration	-	Perform the service
Trend Micro	Antivirus	Trend Micro Antivirus	Request license / offering service and support
Ubiquiti Networks	Managed Wifi	Ubiquiti UniFi	Offering service and support

Veeam Software	Back-up	Veeam back-up	Request license / offering service and support
Westcon-Comstor NL	Hard-/software delivery	Check Point Firewall	If supplier requires data for delivery of the order
Xink	E-mail signature	Xink	Perform the service
Xolphin	Security	SSL certificate	Perform the service

Tabel 1 - Sub-processors Harbers ICT

Exclusions

This document only applies to cloud- and hosting services that Harbers ICT offers. For on-site server and network administration Harbers ICT only plays an advisory role. Customers are responsible for the security of their network and data.

For some of our services the conditions of a third party apply. In general this includes products that are hosted by third parties whereby Harbers ICT cannot influence security measures. This includes Office 365, where the Microsoft conditions apply.