TRAFICOM
National Cyber Security Centre

16.11.2020

Statement of compliance for the Cybersecurity Label

Structure and directions

The goal of this form is to provide information on the security of an IoT product to NCSC-FI as well as technically inclined users. The form is published as a part of a consumer material kit when a label is granted.

Chapter 1 lists general information of the IoT product and the surrounding ecosystem such as mobile applications and cloud services provided by the vendor or third parties. The sections of chapter 2 list security threats that are relevant to consumers as well as security requirements that, when met, mitigate these threats. Where possible, the requirements are accompanied by tables that may be used as part of the response. Some descriptive texts for describing the security posture of the product are suggested.

The ETSI references within the text are related to provisions in the standard ETSI TS 303 645 "CYBER; Cyber Security for Consumer Internet of Things". The final draft (v2.1.0, 2020-04) is available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

Contact information

Company name:	Polar Electro Oy
Business ID:	0209911-2

TRAFICOM
Finnish Transport and Communications Agency

1 Product description

Describe the product or product family (the "Product") under application, along with ecosystem provided by the vendor or third parties (the "Service") that is relevant for core functionalities of the Product.

Polar Ignite is a waterproof fitness watch with advanced wrist-based heart rate and integrated GPS. Polar Flow is the place where you can see, analyze and understand the data that you’re tracking with your Polar product. Polar Flow is available as a web service and as a mobile app for Android and iOS.

1.1 Support period

The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period (ETSI 5.3-13). Specify the support period and describe how the information can be accessed.

Polar is committed to provide security patches for the product 2 years after the EOL statement.

1.2 Security guidance

The manufacturer should provide users with guidance on how to securely set up their device (ETSI 5.12-2). Specify where the security guidance is available in Finnish.

Security guidance for the product is available at Polar website.
https://support.polar.com/fi/ignite

TRAFICOM
Finnish Transport and Communications Agency

1.3 Other certifications

Specify other certifications are requirements the product fulfills. As an example, the product has a CE marking and/or FCC label; the product is has certification X (e.g. the UK security label, provide link); the service components of the product have been verified by Y (provide link); have certification Z (e.g. the STAR certification from the Cloud Security Alliance, provide link).

URL https://www.polar.com/en/regulatory_information will include all certifications Polar products have

2 Protections against common IoT threats

The Product has protections for common IoT threats as described by the following sections.

2.1 Weak, Guessable, or Hardcoded Passwords

Requirement regarding passwords is as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compliant
Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user (ETSI 5.1-1).	☒	☐	☐	☐

TRAFICOM
Finnish Transport and Communications Agency

Describe how the Product is protected against the threats caused by weak or hardcoded passwords. As an example, if the threat is compensated by using security controls beyond identification, or if user identification does not use passwords, describe how the resulting security level is equal to using strong and unique passwords.

Product itself doesn't have passwords. Security guidance includes instructions for creating solid password for Flow service. User is instructed to understand the sensitivity of the data wrist unit has and protect it accordingly.

2.2 Use of Insecure or Outdated Components

Requirement regarding insecure or outdated components are as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compliant
When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates (ETSI 5.3-2).	☒	☐	☐	☐
An update shall be simple for the user to apply (ETSI 5.3-3).	☒	☐	☐	☐
Updates shall be timely (ETSI 5.3-8).	☒	☐	☐	☐
The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update (ETSI 5.3-11).	☒	☐	☐	☐
The manufacturer shall make a vulnerability disclosure policy publicly available (ETSI 5.2-1).	☒	☐	☐	☐
Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period (ETSI 5.2-3).	☒	☐	☐	☐

Finnish Transport and Communications Agency

Describe how the Product and Service are protected against the threat of insecure or outdated components. As an example, describe how vulnerability follow-up is performed throughout the supply chain for all the components, including operating systems, network services and software libraries. Describe how timeliness, ease of installation, quality control and secure transfer and installation is ensured in updates of the Product. Typical update cycles range from 30 to 90 days, though this may vary greatly depending on the nature of the product.

Hotfixes and vulnerabilities will be patched with Polar hotfix process. When there is update, user is informed via FlowSync desktop application or FlowApp mobile application. Updating the product doesn't require any other user action than clicking "Ok" to the update dialog. Polar has security@polar.com and privacy@polar.com email addresses as well as global customer care as contact points.

2.3 Insufficient Privacy Protection

Requirement regarding privacy protection is as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compliant
The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers (ETSI 6.1).	☒	☐	☐	☐

TRAFICOM
Finnish Transport and Communications Agency

Describe how it is ensured that the handling and storage of personally identifiable information (PII) within the Product and the Service is performed in a manner that is transparent to the user and limited to the extent necessary for providing the functionality.

Polar products are GDPR compliant. Privacy related information can be found from URL https://www.polar.com/fi/legal/privacy-notice. User is instructed to understand the sensitivity of the data wrist unit has and protect it accordingly.

You can describe the personally identifiable information (PII) in the following table. Listing the PII will help in their evaluation.

PII	Product/Service/ Component	Purpose	Data Processor

2.4 Insecure Data Transfer and Storage

Requirements regarding data transfer and storage are as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compliant
Sensitive security parameters in persistent storage shall be stored securely by the device (ETSI 5.4-1).	☒	☒	☐	☐
The consumer IoT device shall use best practice cryptography to communicate securely (ETSI 5.5-1).	☒	☐	☐	☐
The manufacturer shall follow secure management processes for critical security parameters that relate to the device (ETSI 5.5-8).	☒	☐	☐	☐

TRAFICOM
Finnish Transport and Communications Agency

Describe how the Product and the Service, as well as the communication between the Product and the Service, are protected against the threats caused by lacks in data encryption and access control. For protecting passwords, this typically includes the usage of hash functions.

Data transfer between wrist device and mobile device require pairing and leverages native BLE encryption scheme. Data transfer between mobile device and ecosystem backend leverages TLS 1.2 protocol. Wrist unit does not store credentials. Wrist unit has secure storage for device specific security keys. Mobile device leverages platform encryption which is usually enabled by default. User must deliberately make a choice of not enabling encryption when taking the device into use.

2.5 Insecure Network Services and Ecosystem Interfaces

Requirements regarding network services and ecosystem interfaces are as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compliant
Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication (ETSI 5.5-5).	☐	☒	☐	☐
All unused network and logical interfaces shall be disabled (ETSI 5.6-1).	☐	☒	☐	☐
Software should run with least necessary privileges, taking account of both security and functionality (ETSI 5.6-7).	☐	☒	☐	☐
The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices (ETSI 5.13-1).	☒	☐	☐	☐

Describe how the Product is protected against the threats caused by the vulnerabilities in the exposed network services such as web interfaces and remote management. Also consider the used radio interfaces.

TRAFICOM
Finnish Transport and Communications Agency

Describe how the exposed network interfaces in the Service, are protected against threats such as unauthorized access and breaches of confidentiality. These interfaces are typically related to functionalities such as the cloud-based data storage and management of the Product.

Wrist unit does not have a TCP stack so there are no open network ports. Data entered via wrist unit UI is valid "by-design" (selectable from list of options). Data entered via Web or Mobile UI is validated before storing. Penetration testing has been conducted to backend to validate that only necessary ports are open. Backend is protected by firewalls, load balancers and DDoS protection appliances.

You can use the following table in your response to sections 2.4 and 2.5. Listing the tools and methods used to test the Product and the Service will help in their evaluation.

Network port / Radio technology	Encryption / access control	Usage
Bluetooth Low Energy	Numeric key comparison	data transfer between wrist unit and mobile device
tcp/443	TLS 1.2	data transfer between mobile device and web backend

2.6 Insecure Default Settings

Requirement regarding insecure default settings is as follows. State the compliancy for the requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compliant
Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability (ETSI 5.12-1).	☒	☐	☐	☐

Finnish Transport and Communications Agency

Describe how the Product and the Service are protected against the threats caused by insecure factory or default settings. Also describe how the user is guided to maintain a secure configuration.

Wrist unit does not have any relevant security related settings as default, it works completely as a standalone unit. Flow default settings are all private on default by GDPR requirements. User guidance happens in Flow service if user wants to change privacy settings.