1) EICAR Minimum Standard for IT Security products

a. To claim adherence to the EICAR Minimum Standard an IT Security Product shall fulfil the following requirements:

i. The requirements in this standard apply to all parts of the product including:

1. Code developed by the vendor
2. Code developed by external parties and included in the product by the vendor
3. Code run on the user's device
4. Backend systems operated by the vendor to the extent they store or process data received from the user's device

ii. The vendor shall have a sufficient understanding of all code in the product, both internally and externally developed, to be able to ensure compliance with this standard.

iii. The vendor shall have sufficient control over all parts of the product's code, both internally and externally developed, to make sure that any discovered faults that conflict with this standard can be amended promptly.

iv. The vendor shall publish a Privacy Declaration covering the product. This declaration is written in a clear and comprehensive way and does not obfuscate relevant information. It contains at least the items mentioned elsewhere in this standard and is kept up to date when new versions of the product is released.

v. The product is designed to fulfil solely its claimed objectives; the claimed objectives are fully described in the product's Privacy Declaration

vi. The vendor does not support any scheme that requires the non-detection of malicious activities.

vii. The product does not contain any hidden functionality or any other intended functionality that is not anticipated by the claimed objectives.

Formatiert: Hervorheben

Kommentiert [RF1]: Check for HW (chips)

Kommentiert [RF2]: Needs review considering research results (Marcel Eberling)

Kommentiert [RF3]: Needs review considering research results (Marcel Eberling)

Kommentiert [RF4]: Needs review considering 0-day bugs

Kommentiert [RF5]: Needs review considering research results (Marcel Eberling)
(Impossible to prove "non-existence of code)

Kommentiert [RF6]: Needs review considering verification (possibly source-code evaluation)

Kommentiert [RF7]: This should be required for Facebook

Kommentiert [RF8]: Define malicious

Kommentiert [RF9]: Needs review considering research results (Marcel Eberling)
(It's only possible to test known malware)

Kommentiert [RF10]: Needs review considering research results (Marcel Eberling)
(It's only possible to prove non-existence of code parts)

Kommentiert [RF11]: Needs review considering verification

Kommentiert [RF12]: Clarify with "third party access schemes"

Kommentiert [RF13]: Consider "positive" wording "only does what it is designed

viii. More specifically, the product does not contain any “back door”* and the vendor does not support any “Third Party Access (TPA)” scheme.

ix. The product uses cryptographic methods to protect data that is transferred to and from the device. The vendor uses cryptographic methods to ensure the integrity of any code or data installed on the user’s devices as part of the product. Any used cryptographic method is based on algorithms and protocols that are considered to be of sufficient strength. Code providing cryptographic algorithms and protocols is either based on widely accepted crypto libraries or otherwise engineered to provide sufficient security and be of sufficient quality.

x. Information identifying the device owner, the product license owner or any other person using the device must not be transferred to the vendor unless there is a compelling reason. The Privacy Declaration shall state if such data is transferred, to what extent and for what reason.

xi. User-owned content, like contacts, messages and documents, must not be transferred to the vendor without the user’s explicit consent. The Privacy Declaration shall state if such data is transferred, to what extent and for what purpose.

xii. Technical information, like device configuration, information about installed and run applications, the application files, usage of features in the product or the system, installed updates and other similar data, can be uploaded to the vendor if that is beneficial for fulfilling the product’s intended purpose and isn’t in conflict with any significant user interest. The Privacy Declaration shall state if such data is transferred, to what extent and for what reason.

xiii. Any data collected from the user’s device is protected in accordance with applicable legal data protection requirements. The Privacy Declaration shall state what or which countries data from the user’s device may be stored in.

Kommentiert [RF14]: Needs review considering research results (Marcel Eberling)
It’s not possible to prove that the vendor did not include any backdoors

Kommentiert [RF15]: ??? GDPR

Kommentiert [RF16]: Clarify meaning with GDPR

Kommentiert [RF17]: To be reviewed considering GDPR requirements and conceivable access to data transferred using encryption or proprietary data formats.

Gelöscht: reason

Kommentiert [RF18]: Review for precision (wording and meaning)

Kommentiert [RF19]: Needs review considering GDPR

Kommentiert [RF20]: Needs review considering research results (Marcel Eberling)
(reliance on vendors statement)

xiv. Authority access to user data stored under the vendors control is solely provided in accordance with current laws.

b. The owner/vendor of the product agrees to be subject to an independent evaluation and verification of the above identified requirements.

*"back door" in the sense of the EICAR Minimum Standard means any, published or non-published access to the application or its code other than the access described with the claimed objectives.

Kommentiert [RF21]: Clarify with Forgo storage out side EU juristictions (Anastasia)

Kommentiert [RF22]: Can we be more precise? (who's law)

Kommentiert [RF23]: Needs review considering GDPR

Kommentiert [RF24]: Needs review considering research results (Marcel Eberling) (reliance on vendors statement)

Kommentiert [RF25]: Needs thorough review considering trust in source-code evaluation

Kommentiert [RF26]: