# The Standard

Below is the current version of the Digital Standard. You can click on the Test Name to view and comment on a section on Github. There you can propose a change, run a test and report results, or start a conversation about how to tackle one of the open questions. **Please note that you will need to be logged into your GitHub account to see the GitHub pages.**

Each criteria has been color-coded to help direct your contribution and participation.

: Well understood with a developed testing approach in place.

: Under development with some outstanding questions.

: Under discussion, usually due to the sensitivity and complexity of the issue.

| Test Name | Criteria | Indicators | Procedure Overview |
|---|---|---|---|

## Security - is it safe?

| Test Name | Criteria | Indicators | Procedure Overview |
|---|---|---|---|
| **Build Quality** | | | |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | **Best Build Practices** | The software was built and developed according to the industry's best practices for security. | The product was built with effectively implemented safety features.<br><br>The software does not make use of unsafe functions or libraries.<br><br>The software is not overly complex. | Run static analysis software to determine what application armoring features are present.<br><br>Are there Stack Guards, and if so, are they effectively implemented?<br><br>Are all safety features available in the pertinent OS enabled? (e.g., ASLR, CFI, RELRO, DEP, etc.)<br><br>Are those safety features well implemented and/or enabled with optimal settings? (E.g., High Entropy ASLR, rather than just Dynamic Base on Windows 10)<br><br>Are the binaries 32 or 64 bit?<br><br>Pull out data from the binary that speaks to developer hygiene.<br><br>Do they use strcpy and | |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | | | | other historically unsafe functions?<br><br>Did the developers use older, less historically safe functions, or newer, safer replacements for those functions?<br><br>What risks are introduced via the libraries that the binary links to, either directly or indirectly?<br><br>Pull out data from the binary that speaks to code complexity.<br><br>What is the branch density?<br><br>How many stack adjusts, function calls, etc are there?<br><br>How complex is the code? | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
|  **Product stability** | The software is reliable. | The software is not susceptible to crashes.<br><br>If the program is forced to unexpectedly terminate, it shuts down in a safe and responsible fashion.<br><br>The software is not vulnerable to algorithmic complexity attacks. | Fuzz software to see if and how it crashes.<br><br>Under appropriate fuzz testing, what was the code coverage, number of crashes, and type(s) of crashes.<br><br>Are crashes exploitable, or do they simply allow a disruption of service?<br><br>Perform modified fuzzing to determine the software's vulnerability to algorithmic complexity attacks. |
| **Data security** | | | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ Bug bounty program | The company is willing and able to address reports of vulnerabilities. | The company has a mechanism through which security researchers can submit vulnerabilities they discover.<br><br>The company discloses the timeframe in which it will review reports of vulnerabilities.<br><br>The company commits not to pursue legal action against security researchers. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| **Encryption** | Information I provide is encrypted so that it can't be easily read or used by attackers. | Transmission of user communications is encrypted by default.<br><br>Transmission of user communications is encrypted using unique keys.<br><br>Users can secure their content using end-to-end encryption.<br><br>End-to-end encryption is enabled by default. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses.<br><br>Inspect traffic to determine if SSL encryption is used. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| **Known Exploit Resistance** | The product is protected from known software vulnerabilities that present a danger from attackers. | The software is secure against known bugs and types of attacks. | Browsers:<br><br>Identify publicly known vulnerabilities for each browser.<br><br>Use the original proof of concept code (if known) or devise custom code where necessary, to test the browser for the issue identified in the vulnerability notice.<br><br>Check if the browser is now protected from the identified vulnerabilities.<br><br>Apps:<br><br>Root/jailbreak the device, configure web proxy and network traffic monitor.<br><br>Launch target app, create accounts, sign-in, launch any activities available from user interface. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| | | | Monitor communication between the application on the device and any backend services.<br><br>Examine file system, database, and logs on the mobile device to determine if sensitive information is stored in a way that could lead to compromise of user data.<br><br>Connected Devices:<br><br>Check if using latest version of software.<br><br>Configure web proxy and network traffic monitor.<br><br>Create account and sign-in to the installed ""out of the box"" applications.<br><br>Launch any activities available from the user interface. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| | | | Monitor communication between the applications on the device, the device itself, and any backend services.<br><br>Examine file system, database, and logs to determine if sensitive information is stored in a way that could lead to compromise of user data." |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| Password | A product which uses a password requires the user to set a good password. | A product which requires password access must have a user-defined or unique password in order to function.<br><br>Passwords are required to be of a certain length.<br><br>Passwords are required to be of a certain complexity.<br><br>The existing password is needed to change the password. | Set up the product and, if a password is used, note whether a password must be selected by the user or the quality of a default password if provided.<br><br>"Note if there are requirements for the password to be at least a certain length.<br><br>Note if there are limitations on how long the password can be."<br><br>Note if the product requires the password to be of a certain complexity (types of characters, prohibiting repeated characters, etc.)<br><br>Note if the product requires knowledge of the existing password in order to execute a password change. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ Security oversight | The company is a responsible caretaker of my data. | The company has systems in place to limit and monitor employee access to user information.<br><br>The company has an internal security team that conducts security audits on the company's products and services.<br><br>The company commissions third-party security audits on its products and services. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
|  **Security over time** | The product is kept protected with software updates. | Automatic software updates<br><br>Notification of software updates<br><br>Ease of installation of software updates<br><br>Software can be kept up-to-date for security issues. | Examine software settings and product documentation to determine if automatic software updates are enabled by default or can be enabled by the user.<br><br>If updates are not automatic, examine software settings and product documentation to determine if the product notifies the user if a software update is available, and if that notification is persistent, or if the user can easily determine if a software update is available.<br><br>Execute the procedure to install a software update and evaluate the ease of installation by comparing against established references.<br><br>Check if a later version of software exists but the product cannot be |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | | | | updated to it (e.g. Android devices with pre-KitKat versions). | |
| | **User Safety** | | | | |
| | ! Personal safety | The company helps me protect myself from grief, abuse, and harassment. | | | |

# Privacy (Is it private?)

| | | | | | |
|---|---|---|---|---|---|
| | **Access and Control** | | | | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ Data control | I can see and control everything the company knows about me. | Users can control the collection of their information.<br><br>Users can delete their information.<br><br>Users can control how their information is used to target advertising.<br><br>Clear explanation of how users can control whether their information is used for targeted advertising.<br><br>Users can obtain a copy of their information.<br><br>Disclosure of what user information users can obtain<br><br>Users can obtain their information in a structured data format.<br><br>Users can obtain all public-facing and private user information the company hold about | Investigation and analysis of publicly available documentation to determine what the company clearly discloses.<br><br>Look in the product's user interface to see what privacy controls exist and what the options are. If relevant, analyze network traffic to see if they are effective. |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | | | them.<br><br>Privacy controls exist and are effective. | | |
| | **Data retention** | | | | |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| ✔ | **Data retention and deletion** | My account and information are deleted when I leave the service.<br><br>I know how long the company keeps my information. | All user information is deleted after users terminate their account or remove service from a device.<br><br>Disclosure of timeframe in which user information is deleted after users terminate their account<br><br>Disclosure of how long each type of user information is retained | Investigation and analysis of publicly available documentation to determine what the company clearly discloses.<br><br>Terminate a test account, remove service from a device, or perform a factory reset on the device.<br><br>Determine whether any information from the test account is still available. (Readiness flag: 3)<br><br>Investigation and analysis of publicly available documentation to determine what the company clearly discloses. | |

## Overreach - Collecting Too Much Data

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| Data benefits | Every piece of data I share brings me a benefit; it doesn't just help the company. | | |
| Data collection | I know what user information this company is collecting. | Disclosure of the type of user information collected<br><br>Disclosure of how user information is collected | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |
| Minimal data collection | The only information the company requests from me is what's needed to make the product or service work correctly. | The user information collected is only that which is directly relevant and necessary for the service.<br><br>Product still works when all permissions not relevant to product's functionality are declined. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses.<br><br>Decline permissions not relevant to the product's functionality, verify that product is still functional |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| **Privacy by default** | The default settings in this product prioritize my privacy; to give up privacy, I actually need to change the settings. | Targeted advertising is off by default.<br><br>Transmission of user communications is encrypted by default.<br><br>End-to-end encryption is enabled by default<br><br>User interface settings which are optimal for privacy are set by default. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses.<br><br>Review settings available from the user interface, and determine which options would be optimal for privacy considerations.<br><br>Determine whether those options are selected by default. |
| **Third Party Tracking - Data Sharing** | | | |

| Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|
| ✔ Data use | The company explicitly discloses every way in which it uses my data. | Disclosure of what user information is shared<br><br>Disclosure of the types of third parties with which user information is shared<br><br>Disclosure whether user information could be shared with government or legal authorities<br><br>Third party domains contacted by the product are named in the privacy policy. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses.<br><br>Analyze network traffic to see if any third party domains are contacted by the product, investigate privacy policy to see which companies, if any, they name. | |

# Governance & Compliance (Are they good?)

### Business Model

| | | | | |
|---|---|---|---|---|
| ! Business model | I understand how the company earns its revenue. | | | |

| Test Name | Criteria | Indicators | Procedure Overview |
|---|---|---|---|
| **Human Rights & Corporate Social Responsibility** | | | |

| Test Name | Criteria | Indicators | Procedure Overview |
|---|---|---|---|
| Governance | The company or organization publicly commits to respect users' human rights to freedom of expression and privacy.<br><br>The company or organization's senior leadership exercises oversight over how its policies and practices affect freedom of expression and privacy.<br><br>The company or organization should have mechanisms in place to implement its commitments to freedom of expression and privacy internally.<br><br>The company or organization implements due diligence processes, such as human rights impact assessments, to identify how all aspects of its activities affect freedom of expression | Explicit and clearly articulated policy commitment to human rights, including freedom of expression and privacy<br><br>The board of directors exercises formal oversight over how company practices affect freedom of expression and privacy.<br><br>An executive-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy.<br><br>A management-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy.<br><br>Provides employee, volunteers or other staff | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | | and privacy and to mitigate any risks posed by those impacts.<br><br>The company or organization engages with a range of stakeholders on freedom of expression and privacy issues.<br><br>The company or organization should have grievance and remedy mechanisms to address user's freedom of expression and privacy concerns. | training on freedom of expression and privacy issues<br><br>Maintains a whistleblower program through which employees, volunteers or other staff can report concerns related to how the company treats its users' freedom of expression and privacy rights<br><br>As part of its decision-making, considers how laws affect freedom of expression and privacy in jurisdictions where it operates<br><br>Regularly assesses free expression and privacy risks associated with existing products and services<br><br>Assesses free expression and privacy risks associated with a new activity, including the | | |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | | | launch and/or acquisition of new products or services or entry into new markets<br><br>Assesses free expression and privacy risks associated with the processes and mechanisms used to enforce its Terms of Service<br><br>Conducts in-depth due diligence wherever the company's risk assessments identify concerns<br><br>Senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in decision-making for the company<br><br>Conducts assessments on a regular schedule | | |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | | | The company initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people directly and adversely impacted by the company's business<br><br>Clear disclosure of processes for receiving complaints<br><br>Process includes complaints related to freedom of expression and privacy<br><br>Clear disclosure of process for responding to complaints<br><br>The company reports on the number of complaints received.<br><br>The company provides evidence that it is responding to complaints. | | |

| Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|
| **Open** | | | | |
| Open Innovation | The company works to advance all technology and innovation, not just its own interests. | | | |
| Open Source | The product's software is publicly available. | Software is open source. | Determine if code is available.<br><br>Determine type of open source license. | |
| **Privacy Policy & Terms of Service** | | | | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| **Terms of Service and Privacy Policy documents** | I can easily find, read, and understand the privacy policy and/or terms of service. | The Terms of service (ToS) are easy to find.<br><br>The ToS are available in the language(s) most commonly spoken by the company's users.<br><br>The ToS are presented in an understandable manner.<br><br>The privacy policies are easy to find.<br><br>The privacy policies are available in the languages(s) most commonly spoken by the company's users.<br><br>The privacy policies are presented in an understandable manner. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ ToS & Privacy Policy change notification | The company provides clear notification when it changes its privacy policy and/or terms of service. | Commitment to notify users about changes to the terms of service<br><br>Disclosure of how users will be directly notified of changes to the terms of service<br><br>Disclosure of timeframe for notification prior to changes to the terms of service coming into effect<br><br>Maintains a public archive or change log of the terms of service<br><br>Commitment to notify users about change to the privacy policy<br><br>Disclosure of how users will be directly notified of changes to the privacy policy<br><br>Disclosure of timeframe for notification prior to changes to the privacy policy coming into effect | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| | | Maintains a public archive or change log of the privacy policy | |
| **Transparency** | | | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ 3rd party requests for user data | The company complies only with legal and ethical third-party requests for user information. | The company explains its process for responding to non-judicial government requests.<br><br>The company explains its process for responding to court orders.<br><br>The company explains its process for responding to requests from foreign jurisdictions.<br><br>The company explains its process for responding to requests made by private parties.<br><br>The company's explanations include the legal basis under which it may comply.<br><br>The company commits to carry out due diligence on requests before deciding how to respond and to push back on unlawful requests. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| | | | The company provides guidance or examples of implementation of its process. | | |
| | ✔ Identity policy | I can register using any name and identifying characteristics I wish, or keep my identity completely anonymous. | The company does not require users to verify their identity with their government-issued identification, or with other forms of identification that could be connected to their offline identity. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ Threat Notification | The company notifies appropriate authorities and those affected when a data breach occurs. | The company will notify the relevant authorities without undue delay when a data breach occurs.<br><br>The company clearly discloses its process for notifying data subjects who might be affected by a data breach.<br><br>The company clearly discloses what kinds of steps it will take to address the impact of a data breach on its users. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ Transparency reporting | The company is transparent about its practices for sharing user data with the government and other third parties. | The company lists the number of requests it receives by country.<br><br>The company lists the number of requests it receives for stored user information and for real-time communications access.<br><br>The company lists the number of accounts affected.<br><br>The company lists whether a demand sought communications content or non-content or both.<br><br>The company identifies the specific legal authority or type of legal process through which law enforcement and national security demands are made.<br><br>The company includes requests that come from | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| | | court orders.<br><br>The company list the number of requests it receives from private parties.<br><br>The company lists the number of requests it complied with, broken down by category of demand.<br><br>The company lists what types of government requests it is prohibited by law from disclosing.<br><br>The company reports this data at least once per year.<br><br>The data reported by the company can be exported as a structured data file. | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ User notification about third-party requests for user information | The company tells me if the government or other third parties ask for my information. | The company notifies users when government entities (including courts or other judicial bodies) request their user information.<br><br>The company notifies users when private parties request their user information.<br><br>The company clearly discloses situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

# Ownership (Is it mine?)

| Ownership |
| --- |

| Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|
| ! Interoperability | The company does not prohibit use of the product with other, complementary, products. | The manufacturer does not use software, copyright, or other devices to restrict the use of products and services that would otherwise be possible to use with your existing products (e.g., set-top boxes, third party applications, etc.). | | |
| ! Ownership | When I buy a product, I own every part of it. | The company does not retain any control or ownership over the operation, use, inputs, or outputs of the product after it has been purchased by the consumer. | | |

| | Test Name | Criteria | Indicators | Procedure Overview |
|---|---|---|---|---|
| ! | **Resale** | I can resell the product to someone and it will still work. | If a consumer sells the product on the private market, the new owner has access to the full functionality of the original product.? Or does the company restrict the transfer of ownership<br><br>The company does not restrict the transfer of ownership. | |
| | **Permanence** | | | |

| | Test Name | Criteria | Indicators | Procedure Overview | |
|---|---|---|---|---|---|
| ! | **Functionality Over Time** | The company will continue to maintain the intended functionality of the product over the product's expected life cycle. | Every feature of the product will continue to work for as long as I can reasonably expect; that is, the manufacturer will not 'brick' certain parts of the product during that time frame.<br><br>The manufacturer will not cease to support the functionality I come to expect.<br><br>Replacement services will exist if the manufacturer ceases to support the functionality. | | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| ✔ **Process for terms of service enforcement** | I know how, when, and why the company or organization unilaterally closes user accounts. | The company or organization clearly explains what types of activities it does not permit.<br><br>The company or organization clearly explains why it may restrict a user's account.<br><br>The company or organization clearly discloses the mechanisms it uses to identify accounts that violate the rules.<br><br>The company or organization clearly discloses whether any non-government and non-judicial entities receive priority consideration when identifying accounts to be restricted for violating the company's rules, and if so, how that priority status is conferred. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| | | The company or organization clearly explains its process for enforcing its rules.<br><br>The company or organization provides clear examples to help the user understand what the rules are and how they are enforced. | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
|  **Transparency about Terms of Service enforcement** | I know how often the company or organization unilaterally closes user accounts | The company or organization publishes data about the number of accounts it restricts or closes on its own initiative.<br><br>The company or organization publishes data about the number of accounts it restricts or closes as a result of a government request.<br><br>The company or organization publishes data about the number of accounts it restricts or closes as a result of a request from private third-parties.<br><br>The company or organization clearly discloses that it notifies users when it restricts or closes user accounts. | Investigation and analysis of publicly available documentation to determine what the company clearly discloses. |
| **Right to Repair** | | | |

| Test Name | Criteria | Indicators | Procedure Overview |
| --- | --- | --- | --- |
| **Repair Accessibility** | The product can be fixed by parties other than the manufacturer. | The company does not use technical, feature-level, or legal means to block a consumer's ability to get a device repaired.<br><br>There is a competitive market of repair shops.<br><br>Repair shops, other than the manufacturer's, are supported by the original manufacturer. | |
| **Repair Penalty** | I am not penalized for getting the product properly repaired by a third party or for repairing it myself. | The company does not penalize consumers (voided warranty, etc.) if they get the product repaired by someone other than the original manufacturer or their authorized representatives. | |