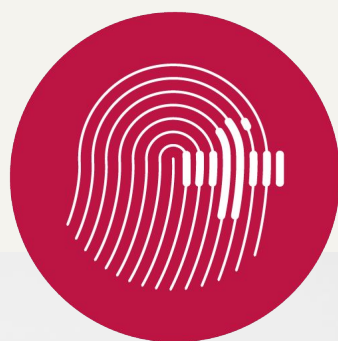




Digital Trust Criteria



SWISS 
DIGITAL
INITIATIVE



Our Digital Trust Criteria

This document shows how the Swiss Digital Initiative defines Digital Trust. As the result of two years of development by a group of experts led by the EPFL, taking into account existing standards and regulations, we have created [a list of 35 criteria along four dimensions \(listed below\)](#) that need to be fulfilled in order for a digital service to receive our [Digital Trust Label](#).

These criteria are listed in full below and also formed the basis for our other digital trust projects like our Digital Trust Compass and the Digital Trust Guide.

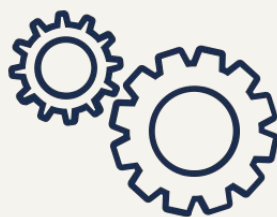
Our Digital Trust Expert Group continually improves these criteria to ensure that we stay at the forefront of digital trust expertise. This is the version of the criteria that are currently valid. Older versions as well as a change log are available on our [website](#).



Security



Data Protection



Reliability



Fair User
Interaction



Security

The criteria in this dimension cover:

- **Secure communication, data transmission & storage**
- **Secure user authentication**
- **Secure service set-up, maintenance and update**
- **Monitoring & reporting of vulnerabilities & breaches**

-
1. The service shall apply best practice cryptography to data in transit, ensuring that the cryptography is reviewed and evaluated, delivers the required functions for all transmitted data and is appropriate to the properties of the technology, risk, and usage. All data in transit over open communication lines such as the internet must be encrypted.
 2. The service shall apply best practice cryptography to data at rest, ensuring that the cryptography is reviewed and evaluated, delivers the required functions for all sensitive and applicable data at rest and is appropriate to the properties of the technology, risk, and usage.
 3. Privacy-enhancing technologies such as Anonymization and Pseudonymization shall be used according to best practices in order to adequately protect the user's data.
 4. All passwords used for the service shall be subject to a state-of-the-art password policy, which includes requirements applicable to the service and ensures that no hard-coded passwords are used, best practice authentication is in place and ensures that brute-force attacks on authentication mechanisms are not feasible.



Security

5. Guidance for secure installation, configuration, and updates shall be in place and updated for each release if necessary. Guidance shall be available in a manner that is easy to access and understand. Any major changes shall lead to a communication to the users in an easy-to-understand format.
6. All software components shall be updatable in a secure manner, and verification of security updates shall be in place.
7. Updates shall be timely. Updates addressing critical security vulnerabilities must be available as soon as possible.
8. Hard-coded critical security parameters in service software source code shall not be used.



Security

9. Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated service software shall be unique per service and shall implement security measures to protect the integrity and confidentiality of critical security parameters.
10. The service provider shall follow secure management processes for critical security parameters that relate to the service.
11. The service provider shall continually monitor, identify, and rectify security vulnerabilities and/or breaches, and shall provide a public point of contact as part of a vulnerability disclosure policy so that security researchers and others are able to report issues.
12. Critical security vulnerabilities shall be communicated to relevant authorities within 72 hours if not corrected, and the impacted users shall be timely and adequately informed. Personal data breaches shall be communicated to relevant authorities and impacted data subjects within 72 hours.



Data Protection

The criteria in this dimension cover:

- **User consent**
 - **Data retention & processing**
-

13. The user shall be informed about the purpose of the processing and the legal basis for processing of their personal data in clear and plain language. Where there is more than one purpose/legal basis, they need to be listed separately in a way that the user is able to easily distinguish between one purpose/legal basis and another.
14. Where user consent is sought for the processing of personal data, such consent shall be expressly collected from the user for each of the purposes and legal basis listed by the service provider and obtained separately from the terms and conditions of use of the services.
15. Where initial user consent is sought for the processing of personal data, the user shall be provided with the option of either opting in, or opting out, expressed through a valid and affirmative action. If checkboxes are used, they shall not pre-ticked. The user shall also be given the possibility of requesting additional information.
16. The user shall be provided with a separate, easy, and accessible way of withdrawing consent.



Data Protection

17. The user shall be informed of the definite time period for which the personal data will be stored. If that is not possible, the user shall be informed of the criteria and reasons used to determine the indefinite period, and a regular timeframe for which a review will be undertaken.
18. In cases in which the service provider anonymises personal data, upon a request by the user, such service provider shall provide a detailed explanation of how personal data is being anonymised, and the safety measures used to prevent de-anonymisation. The service provider shall also update the user on the anonymisation status of any personal data held by the provider at the time of the request.
19. Once the data retention period lapses, the service provider shall either anonymise or delete the personal data. In case of indefinite data retention periods where regular reviews are to be undertaken (criteria 17), the user shall be informed of the outcomes of the review within 30 days.
20. The service provider shall ensure that the user can access their data. Any requests for access need to be acceded to within 30 days. Together with a copy of the personal data, a user is to be provided with names of third parties with whom such personal data has been shared, together with the legal basis under which such data is being held.

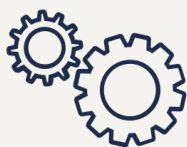


Reliability

The criteria in this dimension cover:

- **Reliable service updates**
- **Resilience to service outage**
- **Functional reliability**
- **Accountability**

-
21. The software version of the service shall be easy to access and understand.
 22. The service provider shall publish, in a way that is easy to access and understand for the user, the defined support period and the need for that support period.
 23. Disaster recovery, business continuity and data backup and restore policies and procedures shall be in place and regularly tested to ensure ongoing availability of the service and associated data.
 24. The service shall provide its users with an extensive, easy-to-access, easy-to-understand description of its functionalities, and shall operate in strict accordance with this description.



Reliability

25. If relevant, the service shall provision for a secure, precise and efficient billing and payment system which employs two-factor authentication and adheres to local and regional norms.
26. If relevant, the service shall provision for a delivery system which fulfills state-of-the-art conditions of the associated specific activity domain.
27. The service shall provide its users with an easy-to-access, easy-to-understand, and easy-to-print service and service provider identification.
28. The service shall document its compliance with all applicable laws and regulation and assign a contact representative for easy-to-access and easy-to-understand information about legislation that the service is subject to.
29. User inquiries and complaints shall be treated in a timely fashion, and relevant alternative dispute resolution mechanisms must be in place to facilitate these processes.



Fair User Interaction

The criteria in this dimension cover:

- **Non-discriminating access**
- **Fair user interfaces**
- **Fair use of AI-based algorithms**

-
30. The system shall provide a non-discriminating access to all its potential users.
 31. Service interfaces shall be designed so as not to deceive, nor to manipulate the users, and, in particular, shall exclude clearly manipulative techniques ("dark patterns") such as Interface Interference (Preselection, Obstruction), Aesthetic Manipulation (Toying with emotions, False Hierarchy), Disguised ads (Trick questions, Sneaking), Forced Actions (Social Pyramid, Gamification, Privacy Zuckering). In addition, the use of mildly manipulative techniques shall be clearly announced to the users and proportionate to the objectives of the service.
 32. The service shall not be designed to exclusively cause user addiction and shall provide the users with an easy-to-access, easy-to-understand information about potential addiction risks during its set up.
 33. Service providers whose services are illegal to users under the age of 18 shall take proportional steps to verify users' age and prevent under-18s from accessing those services.



Fair User Interaction

34. There shall be clear information to the user when interacting with AI-based algorithms and, especially, with automated decision-making algorithms. The service provider shall also indicate which user-related data is processed by the algorithms and its relationship to the objectives of the service, in addition to informing why an AI is used for the service. Any risks inherent to the algorithms must be clearly and concisely described to the user.
35. If AI-based algorithms and, especially, automated decision-making algorithms, are used, the service shall provision for specific mechanisms to assess their robustness, resilience, and accuracy, as well as the risks associated with their exploitation, and shall provide the user with the possibility to request that a representative of the service provider, reviews and validates the outputs produced by the algorithm.

Appendix

The Digital Trust Criteria is an evolving and living document. As technology develops at the fastest pace ever seen, SDI's Digital Trust Expert Committee is in charge of constantly revising and updating the Criteria to try to keep it as up-to-date as possible.

The Digital Trust Criteria is the base and inspiration of all our projects & trust tools:

- [Digital Trust Label](#) - A first-in-the-world actionable tool to advance digital trust and advance organisation's digital responsibility
- [Digital Trust Compass](#) - online self-assessment tool to determine whether organisations respect and protect the interests of its users and to raise awareness among end-users.
- [Digital Trust Guide](#) - The 'user guide' to digital trust. This guide is designed to assist, be it businesses or organisations that handle user data. The primary objective is to establish a robust framework of trust that safeguards the interests of users.

**TRY OUT OUR UNIQUE TOOLS & EMBRACE
DIGITAL TRUST!**



Visit our [website](#) and check out how you can contribute to the Digital Trust Movement!

If you have any questions, get in touch with us:
info@sdi-foundation.org

DIGITAL TRUST



Disclaimer: This document has been prepared only for purposes of the use of the recipient and only serves for the scope and the terms agreed. This document may not be reproduced or circulated without the Swiss Digital Initiative's prior written consent. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else. © 2022 Swiss Digital Initiative. Digital Trust Label. All rights reserved.