



1 Code of Conduct for Relying Parties for services 2 to Government

3 **Version:** 1.0

4 **Document Date:** 2017-10-02

5 **Editors:** Rainer Hoerbe, Keith Uber

6 **Contributors:** <https://kantarainitiative.org/confluence/x/wQA0>

7 **Produced by:** eGovernment WG

8 **Status:**

9 This document is a Kantara Initiative Report produced by the eGovernment WG. It has been
10 approved by the Leadership Council of the Kantara Initiative. See the Kantara Initiative
11 Operating Procedures at <https://kantarainitiative.org/confluence/x/owVAAg> for more
12 information.

13 **Abstract:**

14 This document (Report: Code of Conduct for Relying Parties) provides supporting guidance
15 to the controlling documents of the Kantara Initiative Identity Assurance Framework (IAF) so
16 that, in the fullness of time, the IAF and its controlling document suite could be extended to
17 include the role of Relying Parties (RPs).

18 **IPR Option:**

19 Creative Commons Attribution Share Alike

20 **Suggested Citation:**

21 *Code of Conduct for Relying Parties for services to Government 1.0*. Kantara Initiative
22 eGovernment WG. 2017-10-02. Kantara Initiative Report. [https://kantarainitiative.org/file-](https://kantarainitiative.org/file-downloads/code-of-conduct-rp-v1-0/)
23 [downloads/code-of-conduct-rp-v1-0/](https://kantarainitiative.org/file-downloads/code-of-conduct-rp-v1-0/)

24

Code of Conduct for Relying Parties for services to Government

25

NOTICE



26

27 This work is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported
28 License (CC BY-SA 3.0). To view a copy of the license, visit
29 <https://creativecommons.org/licenses/by-sa/3.0/>

30

31 You are free to:

32 Share — copy and redistribute the material in any medium or format
33 Adapt — remix, transform, and build upon the material for any purpose, even
34 commercially.

35 This license is acceptable for Free Cultural Works.

36 The licensor cannot revoke these freedoms as long as you follow the license terms.

37 Under the following terms:

38 Attribution — You must give appropriate credit, provide a link to the license, and
39 indicate if changes were made. You may do so in any reasonable manner, but not in
40 any way that suggests the licensor endorses you or your use.

41 ShareAlike — If you remix, transform, or build upon the material, you must distribute
42 your contributions under the same license as the original.

43 No additional restrictions — You may not apply legal terms or technological
44 measures that legally restrict others from doing anything the license permits.

45 Notices:

46 You do not have to comply with the license for elements of the material in the public domain
47 or where your use is permitted by an applicable exception or limitation.

48 No warranties are given. The license may not give you all of the permissions necessary for
49 your intended use. For example, other rights such as publicity, privacy, or moral rights may
50 limit how you use the material.

51

52 For any reuse or distribution, you must make clear to others the license terms of this work.
53 The best way to do this is with a link to this document.

54 Copyright: The content of this document is copyright of Kantara Initiative, Inc.

55 © 2017, 2018 Kantara Initiative, Inc.

Code of Conduct for Relying Parties for services to Government

56	Contents	
57	1 INTRODUCTION	4
58	2 ON CONCEPTUALIZING A TYPICAL TABLE OF CONTENTS FOR A CODE OF	
59	CONDUCT FOR RELYING PARTIES	5
60	3 EXEMPLAR DRAFT TEXT FOR THE TABLE OF CONTENTS HEADINGS ABOVE	
61	SELECTED AND MARKED AS *	6
62	3.1 DATA PROTECTION	6
63	3.2 ADMIN, RECORD KEEPING AND PROCESSES/PROCEDURES	7
64	3.3 EXIT AND OFF BOARDING	9
65	4 REFERENCES	10
66	5 REVISION HISTORY	11

67 **1 INTRODUCTION**

68 This document (Report: Code of Conduct for Relying Parties) provides supporting guidance
69 to the controlling documents of the Kantara Initiative Identity Assurance Framework (IAF) so
70 that, in the fullness of time, the IAF and its controlling document suite could be extended to
71 include the role of Relying Parties (RPs).

72 The intended audience for this document are Trust Framework operators that may require
73 requirements for RPs be specified.

74 A complete Code of Conduct for Relying Parties, that spans the full extent of a RP's policies,
75 processes and procedures, might include Sections such as the following:

- 76 1. Data Protection,
- 77 2. Admin, Record Keeping and Process,
- 78 3. Audit and Compliance,
- 79 4. Exit and Off Boarding and
- 80 5. Marketing.

81 It should be noted that other aspects, applicable to a given context or domain, might be
82 required to make it comprehensive.

83 At this time the document is not intended to be a complete set of requirements for good
84 behaviour of a RP. Rather, it is intended to give pointers to the range of topics that should
85 typically be addressed in describing this set of requirements. A few exemplars have been
86 provided for some of the topics.

87 **2 ON CONCEPTUALIZING A TYPICAL TABLE OF** 88 **CONTENTS FOR A CODE OF CONDUCT FOR RELYING** 89 **PARTIES**

90 This document offers an insight into what a typical Code of Conduct for Relying Parties
91 might contain by presenting a draft Table of Contents. Further, it assumes that the Code of
92 Conduct for Relying Parties would form just one component of a larger document suite (e.g.,
93 the IAF) covering other aspects of federated identity activities.

94 It assumes that the following artefacts and conditions exist in that broader framework
95 document set for the federation:

- 96 1. a set of agreed definitions/terminology,
- 97 2. Scope and specification of the Relying Party activities,
- 98 3. a legal contract in force to make all obligations clear for interpretation,
- 99 4. that a federated trust framework is operating, and
- 100 5. that a quality ISMS is operating in the RP/AP environments.

101 With the above conditions met, a Table of Contents for the Code of Conduct for Relying
102 Parties aspect of the document set might include:

- 103 • Introduction and Purpose
- 104 • Executive Summary
- 105 • Assumptions
- 106 • Definitions/Terminology
- 107 • References and bibliography
- 108 • Activities in scope for the Relying Party
- 109 • Data Protection*
- 110 • Administration, Record Keeping and processes/procedures*
- 111 • Audit and Compliance
- 112 • Exit and Off boarding*
- 113 • Marketing

114 * (note: example text for this topic has been drafted below)

115 3 EXEMPLAR DRAFT TEXT FOR THE TABLE OF 116 CONTENTS HEADINGS ABOVE SELECTED AND 117 MARKED AS *

118 Note: the text in square brackets [...] indicates a principle or objective that the statement
119 seeks to address.

120 3.1 DATA PROTECTION

121 The RP/Service Provider agrees and warrants:

- 122 1. [Legal compliance] to only process the Attributes in accordance with the relevant
123 provisions of the law applicable to the RP/Service Provider/Federation;
- 124 2. [Purpose limitation] to only process Attributes of the End User that are necessary for
125 enabling access to the service provided by the Service Provider;
- 126 3. [Data minimisation] to minimise the Attributes requested from a party to the
127 Federation to those that are adequate, relevant and not excessive for enabling
128 access to the service and, where a number of Attributes could be used to provide
129 access to the service, to use the least intrusive Attributes possible;
- 130 4. [Deviating purposes] not to process the Attributes for any other purpose (e.g. selling
131 the Attributes or selling the personalisation such as search history, commercial
132 communications, profiling) than enabling access, unless prior consent has been
133 given to the Service Provider by the End User;
- 134 5. [Data retention] to delete or anonymise all Attributes as soon as they are no longer
135 necessary for the purposes of providing the service;
- 136 6. [Third parties] not to transfer Attributes to any third party (such as a collaboration
137 partner) except 1. if mandated by the Service Provider for enabling access to its
138 service on its behalf, or 2. if the third party is committed to the Code of Conduct or
139 has undertaken similar duties considered sufficient under the data protection law
140 applicable to the Service Provider or 3. if prior consent has been given by the End
141 User;
- 142 7. [Security measures] to take appropriate technical and organisational measures to
143 safeguard Attributes against accidental or unlawful destruction or accidental loss,
144 alteration, unauthorized disclosure or access. These measures shall ensure a level
145 of security appropriate to the risks represented by the processing and the nature of
146 the data to be protected, having regard to the state of the art and the cost of their
147 implementation.

Code of Conduct for Relying Parties for services to Government

- 148 8. [Information duty towards End User] to provide to the End User, at least at first
149 contact, in an easily, directly and permanently accessible way a Privacy Policy,
150 containing at least the following information:
- 151 1. the name, address and jurisdiction of the Service Provider;
 - 152 2. the purpose or purposes of the processing of the Attributes;
 - 153 3. a description of the Attributes being processed
 - 154 4. the third-party recipients or categories of third party recipient to whom the
155 Attributes might be disclosed, and proposed transfers of Attributes to
156 countries outside of the jurisdiction/federation
 - 157 5. the existence of the rights to access, rectify and delete the Attributes held
158 about the End User;
 - 159 6. the retention period of the Attributes;
 - 160 7. a reference to this Code of Conduct;
- 161 9. [Information duty towards the Federation party/IDP] to provide to it or its Agent at
162 least the following information:
- 163 1. machine-readable link to the Privacy Policy;
 - 164 2. indication of commitment to this Code of Conduct;
 - 165 3. any updates or changes in the local data protection legislation, which are less
166 strict than the principles set out in this Code of Conduct;
- 167 10. [Security Breaches] to, without undue delay, report all suspected privacy or security
168 breaches (including unauthorized disclosure or compromise, actual or possible loss
169 of data, documents or any device, etc.) concerning the Attributes, to the Federation
170 Party/IdP or its Agent;
- 171 11. [Transfer to third countries] when Attributes are being transferred outside the
172 jurisdiction and to countries with adequate data protection pursuant to adequacy
173 law/rules etc. to ensure an adequate level of protection of the Personal Data by
174 taking appropriate measures pursuant to the law of the country in which the
175 RP/Service Provider is established, such as requesting End User consent or entering
176 into agreements with the RP/Service Provider.

177 **3.2 ADMIN, RECORD KEEPING AND PROCESSES/PROCEDURES**

- 178 1. [Payment] pay the Charges in accordance with XXXX clause in the Federation
179 Agreement;

Code of Conduct for Relying Parties for services to Government

- 180 2. [Co-operation] co-operate with Federation/IdP personnel in connection with its
181 background checking/identity proofing of RP/SP responsible officers, registering
182 authorisation policy for and provide access to records and resources, operation and
183 safe-guarding of the Service/s; and advise IdP promptly of any Service anomalies,
184 suspicious or unusual usage, or complaints relating to the Services and provide
185 reasonable assistance to Federation/IdP in the investigation of such anomalies,
186 usage or complaints;
- 187 3. [Standards Compliance] comply with any standards or specifications issued by the
188 Federation/IdP and any reporting obligations required by the IdP/AP from time to
189 time in accordance with any relevant legislation (including those of a contracted third
190 party to the RP/SP)
- 191 4. [Audit] provide appropriate assistance, where reasonably requested by IdP/AP, in
192 carrying out any audit of the Client's use of the Services or related systems or
193 suppliers; comply with all certification and accreditation requirements
- 194 5. [Federation Reporting] participate in progress reporting as specified in the Service
195 Schedule;
- 196 6. [Transparent Relationship] ensure that the agency Service Provider/RP's website
197 terms and conditions explain the inter-relationship of the Services and the Client's
198 systems in terms agreed with Federation/IdP; that the RP/Service Provider maintains
199 an accurate and up to date register of its roles and activities
- 200 7. [Promotion] use its best endeavours to promote the Services and instructions for
201 use, to its customer base to encourage service uptake and use;
- 202 8. [Maintenance and notification] use and maintain the Service Interface including the
203 security between the Client's systems and the Service
204 System; register/modify/remove/retrieve meta-data, maintain PKI certificates as
205 defined in the XX Federation Documentation XX; notify IdP of any network changes
206 or certification renewals that may impact on any part of the Service, use the Admin
207 interface to register and update details relating to the Service and the officers
208 charged with administering the service
- 209 9. [Technical Consistency] Requirements for mandatory conformance testing before
210 being connected to the production environment; Requirements for session
211 management and logout (e.g. requirements for session timeout periods and single
212 logout behaviour across the federation); Requirements for logging certain events
213 (e.g. SAML Request/Responses) and to establish correlation identifiers in logs;
214 Requirements for UI (to ensure a consistent user experience across the federation -
215 e.g. layout and placement of 'logout' buttons etc.); Requirements for certificates used
216 to secure communication between SP and IdP.

217 3.3 EXIT AND OFF BOARDING

- 218 1. [Exit and off boarding] RP must have an explicit written policy to address and
219 mitigate impacts to existing users (e.g portability of accounts if feasible, re-
220 enrollment, credential switching) in the event that the RP terminates or is terminated
221 from its role.
- 222 2. [Exit and off boarding] RP must have predetermined processes to put into action to
223 update Helpdesk on status, call handling procedures and documentation, website
224 information, test scripts and system flows to reflect the terminated state of the RP

225 4 REFERENCES

- 226 GEANT: <http://www.geant.net/uri/dataprotection-code-of-conduct/V1/Pages/default.aspx>
227 (accessed from [https://www.clarin.eu/content/how-can-i-comply-data-protection-code-
conduct](https://www.clarin.eu/content/how-can-i-comply-data-protection-code-
228 conduct))
- 229 Federal Government of Canada: '[Adding and removing Credential Service Providers under
230 the Credential Broker Service](#)' TBS Canada, CIO Branch, Feb 2015, Version 4.0
- 231 Kantara Initiative: [Identity Assurance Framework](#)
- 232 InCommon: <https://www.incommon.org/docs/policies/InCommonFOPP.pdf>
- 233 IETF: Vectors of Trust: [https://datatracker.ietf.org/doc/draft-riche-vec-tors-of-
trust/?include_text=1](https://datatracker.ietf.org/doc/draft-riche-vec-tors-of-
234 trust/?include_text=1) for the latest version, taken
235 from <https://www.ietf.org/mailman/listinfo/vot>
- 236 NZ RealMe: <https://www.realme.govt.nz/>
- 237 TERENA: <https://refeds.terena.org/index.php/Federations>
- 238 NemLog-in Denmark: [http://www.digst.dk/~media/Files/NemLogin/Tilslutnings-doks/Guide-
til-foederationstilslutning-V1-1.pdf](http://www.digst.dk/~media/Files/NemLogin/Tilslutnings-doks/Guide-
239 til-foederationstilslutning-V1-1.pdf)

240 **5 REVISION HISTORY**

241 2017-10-02 Initial Draft