

Security Operational Baseline

Publication Date: 2025-11-14
Authors: David L. Groep (ed.); Alf Moens; Daniel Kouřil; Baptise Grenier; David Crooks; David Kelsey; Ian Neilson; Liam Atherton; Linda Cornwall; Marcus Hardt; Matt Viljoen; Peter Bolha; Pinja Koskinen; Ralph Niederberger; Romain Wartel; Sven Gabriel; and Urpo Kaila

Document Code: AARC-G084
DOI: 10.5281/zenodo.17349890

Framework: Policy Development Kit v2

© by the authors and the AARC Community, 2003-2025



Abstract

The Security Operational Baseline provides a reference set of minimum expectations and requirements of the behaviour of those offering services to users, communities, and other participants in a distributed ecosystem leveraging a federated AAI, and of those providing access to services or assembling service components. It aims to establish a sufficient level of trust between all participants to enable reliable and secure operation.



Table of Contents

Table of Contents..... 2

1. Introduction..... 3

2. Terminology..... 3

3. Security Baseline 4

References 5

Licensing information 5

1. Introduction

To fulfil its mission and protect primary and secondary assets of any infrastructure and community, it is necessary to be protected from damage, disruption, and unauthorised use. This reference 'Security Operational Baseline' supports these goals by defining minimum expectations and requirements of the behaviour of those offering services to users and communities, and of those providing access to services or assembling service components. It aims to establish a sufficient level of trust between all participants in an infrastructure to enable reliable and secure operation.

The Security Operational Baseline codifies current community good practice for protecting authentication providers, AAI platforms, and identity providers, participating in an AAI Federation. It is RECOMMENDED that all service providers follow these Baseline Requirements to achieve a sufficient level of security. These requirements augment but do not replace applicable security policies and obligations, nor any more specific security arrangements and service level agreements that may exist between participants.

2. Terminology

Terminology in this document follows conventional IT service management vocabulary, such as ITIL [ITIL] and FitSM [FITSM], and the RFC 2119 [RFC2119] key words. For clarification, we define the following specific terms.

Term	Definition
Service Provider	an organisation (or part of an organisation) that manages and delivers a service or services to customers
Identity Provider	a service that creates, maintains, and manages identity information for principals and provides authentication services to relying parties
AAI Platform	an authentication/authorization infrastructure (AAI) service or service component, identity, community, infrastructure, or local 'proxy' that augments, translates, or transposes authentication and authorization information, including the connected sources of access (AAI) attributes, as detailed in the AARC BPA 2025 (AARC-G080) .
User	an individual that primarily benefits from and uses a service

This Guideline is accompanied by implementation recommendations and reference material. Links to these materials are provided at <https://aarc-community.org/guidelines/aarc-g084/>.

3. Security Baseline

To adhere to the Security Operational Baseline, you must:

1. comply with the SIRTFI¹ security incident response framework for structured and coordinated incident response
2. ensure that your Users agree to an Acceptable Use Policy (AUP) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
4. honour the confidentiality requirements of information gained as a result of your Service's participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to the personal data processed, and only use access personal data for administrative, operational, accounting, monitoring or security purposes.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security incident (the 'who, what, where, when', and 'to whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
8. operate services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
9. collaborate in a timely fashion with others, specifically those with which there is a direct trust relationship, in the reporting and resolution of security events or incidents related to their participation in the infrastructure and those affecting the infrastructure as a whole.
10. honour the obligations on security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
11. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of the Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline.

¹ <https://refeds.org/sirtfi/>

References

- BPA2025** AARC Community *AARC Blueprint Architecture: initial revision*
<https://aarc-community.org/guidelines/aarc-g080>
- FITSM** FitSM Standards for lightweight IT Service Management, retrieved from
<https://www.fitsm.eu/>, November 2025
- ITIL** ITIL, Information Technology Infrastructure Library, retrieved from
<https://www.itil.com/>, November 2025
- RFC2119** S. Bradner *Key words for use in RFCs to Indicate Requirement Levels* (RFC 2119), retrieved from <https://www.ietf.org/rfc/rfc2119.txt>
- SIRTFI** REFEDS Community *Security Incident Response Trust Framework for Federated Identity v2*, retrieved from <https://refeds.org/sirtfi/>

Licensing information

This AARC Security Operational Baseline in the policy development kit is based upon multiple sources used under CC BY-NC-SA 4.0 license, including the UK “IRIS Service Operations Security Policy” (<https://www.iris.ac.uk/security/>) and the “Service Operations Security Policy” from the AARC Policy Development Kit version 1 (<https://aarc-community.org/policies/policy-development-kit/>) owned by the authors, used under CC BY-NC-SA 4.0, and the EOSC Security Operational Baseline (<https://doi.org/10.5281/zenodo.7396725>).

This AARC G084 Security Operational Baseline is licensed under CC BY-NC-SA 4.0.