Hardening SUSE Linux with OpenSCAP

WHAT?

OpenSCAP is an open source toolset that implements the Security Content Automation Protocol (SCAP) framework. Combined with the SCAP Security Guide (SSG), it enables automated security auditing and hardening of SUSE Linux.

WHY?

Automated scanning and remediation reduce manual effort, ensure consistent policy enforcement across systems, and support compliance with regulations such as HIPAA, PCI-DSS v4 and ANSSI-BP-028.

EFFORT

Reading time: approximately 30 minutes. A full scan and remediation cycle takes 1–2 hours depending on the number of rules and the initial state of the target system. Familiarity with the Linux command line is required.

GOAL

After completing this article, you can install the required packages, select a security profile, scan your system for policy violations, and remediate identified issues automatically or manually.

REQUIREMENTS

- A running installation of SUSE Linux.
- `root` or **`sudo`** privileges on the target system.
- Access to SUSE repositories for package installation, or an offline package source.
- A non-production test environment for validating remediation before applying it to production systems.

Publication Date: 03 Sep 2026

Contents

1 Auditing and hardening SUSE Linux with OpenSCAP 3
2 SCAP and OpenSCAP 3
3 Preparing the IT infrastructure 5
4 Installing OpenSCAP and the SCAP Security Guide 6
5 SSG Content, directories and profiles 7
6 Scanning the system for vulnerabilities 9
7 Remediating vulnerabilities 12
8 For more information 17
9 What's next 18
10 Legal Notice 18
A GNU Free Documentation License 19

1 Auditing and hardening SUSE Linux with OpenSCAP

This article explains how to use OpenSCAP and SSG to audit and harden SUSE Linux systems against recognized security baselines.

The following sections describe how to prepare your environment, install the required packages, select a security profile, scan your system for policy violations, and remediate any issues found. The sections are arranged in the order of a typical hardening workflow, but the scanning and remediation steps can also be performed independently once the prerequisites are in place.

2 SCAP and OpenSCAP

SCAP is a framework of specifications for automating security compliance. OpenSCAP implements this framework for Linux, and together with the SCAP Security Guide, enables automated auditing and hardening of SUSE Linux.

2.1 What is SCAP?

SCAP stands for *Security Content Automation Protocol*. It is a framework of specifications developed and maintained by the National Institute of Standards and Technology (NIST) that supports automated configuration, vulnerability scanning, and policy compliance evaluation of systems in an organization. SCAP also standardizes how vulnerabilities and security configurations are communicated, both to machines and to human beings.

2.2 What is OpenSCAP?

OpenSCAP is a collection of open source tools that implement the SCAP framework for Linux. It received the SCAP 1.2 certification from NIST in 2014. OpenSCAP works together with the `SCAP Security Guide` (SSG), which implements security guidelines recommended by respected authorities in a machine-readable format. This allows OpenSCAP to automatically audit and harden your SUSE Linux system against recognized security baselines.

2.3 Key SCAP components

SCAP consists of the following components, which interact to describe, evaluate and report on the security state of a system.

Open Vulnerability and Assessment Language (OVAL)

An XML format for testing the presence of a specific state on a system.

Extensible Configuration Checklist Description Format (XCCDF)

An XML format that specifies security checklists, benchmarks, and configuration documentation. An XCCDF file contains a benchmark consisting of different profiles, where each profile is a set of rules with OVAL definitions. Profiles correspond to security practices such as HIPAA, PCI-DSS, and ANSSI-BP-028.

Common Platform Enumeration (CPE)

A structured naming scheme maintained by NIST for identifying IT systems, platforms, and software packages. A CPE name has the following format: `cpe:/part:vendor:product:version:update:edition:language`

DataStream (DS)

An XML format that bundles multiple SCAP components (CPE, XCCDF, OVAL) into a single file for distribution over a network. DataStream files are the primary input format for OpenSCAP when hardening and auditing a SUSE Linux system.

Common Configuration Enumeration (CCE)

Unique identifiers assigned to security-related system configuration issues, used to track individual rules across profiles and tools.

2.4 What is the SCAP Security Guide?

The `SCAP Security Guide` is an open source project that provides machine-readable security policies for Linux systems. It translates established security benchmarks, such as Defense Information Systems Agency (DISA) STIGs and Center for Internet Security (CIS) benchmarks, into SCAP content that can be automatically applied and verified. The `SCAP Security Guide` delivers XCCDF checklists, OVAL checks, and ready-to-use remediation scripts in the form of Ansible playbooks and Bash scripts.

2.5 Benefits of using OpenSCAP with the SCAP Security Guide

Using OpenSCAP together with the SCAP Security Guide provides the following benefits:

- Security guidelines from recognized authorities are transformed into a machine-readable format, removing the need for manual interpretation.
- Scanning and remediation can be automated and run repeatedly, ensuring consistent policy enforcement across all systems in your infrastructure.
- Results are stored in standardized XML formats and can be rendered as human-readable HTML reports for audit and compliance purposes.
- Multiple security profiles are available out of the box, covering regulations such as HIPAA, PCI-DSS v4, and ANSSI-BP-028, reducing the effort required to achieve and demonstrate compliance.

3 Preparing the IT infrastructure

Before installing and applying the SCAP Security Guide, prepare your IT infrastructure to ensure a controlled and repeatable hardening process.

3.1 Introduction

Applying security hardening without prior planning can lead to service disruptions, misconfigurations, and incomplete compliance. The steps below help you assess your environment, define the scope of hardening, and set up a safe testing workflow before touching production systems.

3.2 What pre-hardening steps should you follow?

1. Create an inventory of the hosts on which the SCAP Security Guide will be installed.
2. Create an inventory of the IT and business services that will be in scope for the installation.
3. Divide the inventory into groups. Hosts within the same group will share an identical configuration.
4. Select the security standard or profile you plan to implement. For SUSE Linux, the available profiles include ANSSI-BP-028 (at four levels), HIPAA, and PCI-DSS v4. For the full list of supported profiles, refer to *Section 5, "SSG Content, directories and profiles"*.

5. For each group, create a list of rules and recommendations you plan to implement. Consider the following for each rule:
    - Preconditions required by the rule
    - Configuration parameters, if any
    - Whether the rule will be applied manually or automatically
    - Rules to be excluded, and the additional security controls that will compensate for each exclusion
6. Set up a test environment that closely mirrors your production environment. Use it to validate hardening before applying it to production. Keep the following in mind:
    - Run remediation more than once. Rules are applied in alphabetical order. Dependencies exist between some rules, and a system restart is required after each pass.
    - A 100% pass rate is not achievable in practice. Define an acceptable number of non-passing rules for each group, document them, and apply compensating security controls.
7. Use the test environment to validate new patches and updated versions of the SCAP Security Guide before rolling them out.
8. If a rule fails during remediation, consider one of the following approaches:
    - Apply the rule manually.
    - Exclude the rule using a tailoring file and apply a compensating security control instead.
    - File a bug report, including the SCAP Security Guide version, execution logs, and the steps you performed.
9. Create an implementation plan covering your production environment.
10. Create backups of all target systems before proceeding.

4 Installing OpenSCAP and the SCAP Security Guide

Install the core packages required to scan and remediate SUSE Linux with OpenSCAP and the SCAP Security Guide, and optionally install the graphical SCAP Workbench for a GUI-based workflow.

4.1 Installing the core packages

The following two packages are required for all scanning and remediation workflows described in this article:

- `openscap-utils`: provides the **`oscap`** and **`oscap-ssh`** command-line tools.
- `scap-security-guide`: provides the SCAP Security Guide security content, including DataStream files, profiles, fix scripts, and Ansible playbooks.

Install both packages with the following command:

```
> sudo zypper install openscap-utils scap-security-guide
```

4.2 Installing optional packages

The following packages are optional and extend the core workflow:

- `scap-workbench`: a graphical utility for performing common **`oscap`** tasks, including scanning and profile customization. Available only for desktop installations of SUSE Linux.
- `ssg-apply`: used together with SCAP Workbench to conveniently apply a tailoring file for customized hardening.

```
> sudo zypper install scap-workbench ssg-apply
```

Tip: Security best practice for SCAP Workbench

Avoid installing SCAP Workbench on the target system you plan to harden. Instead, install it on a separate client machine and apply hardening to the target system remotely, maintaining an air gap until the target is connected to a potentially insecure network.

5 SSG Content, directories and profiles

Reference information on the SCAP Security Guide directory layout, the content available after installation, and the security profiles supported for SUSE Linux.

5.1 SSG directories and files

After installing the `scap-security-guide` package, the SSG security content is available in the following directories:

`/usr/share/xml/scap/ssg/content/`

Contains the SSG security content in XML format. All files are named according to the SCAP component and the product they apply to. To list all available DataStream files, run:

```
> ls -l /usr/share/xml/scap/ssg/content/ssg-*-ds.xml
```

`/usr/share/doc/scap-security-guide/guides/`

Contains human-readable HTML versions of the profiles. Each guide describes the rules included in a profile, the rationale behind each rule, severity levels, CCE identifiers, and available remediation options. To list all available guides, run:

```
> ls -l /usr/share/doc/scap-security-guide/guides/ssg*.html
```

To view a specific guide in a web browser, for example the `anssi_bp28_high` profile for SUSE Linux, run:

```
> firefox /usr/share/doc/scap-security-guide/guides/ssg-sle16-guide-
anssi_bp28_high.html
```

The same content is also available online as static HTML pages at https://complianceas-code.github.io/content-pages/guides/index.html.

`/usr/share/scap-security-guide/`

Contains fix scripts for remediating vulnerabilities found during a scan, in the following formats:

- Shell scripts: `bash/*.sh`
- Ansible playbooks: `ansible/*.yml`

5.2 Supported profiles for SUSE Linux

The following security profiles are supported by SUSE for SUSE Linux. The profiles are maintained in the ComplianceAsCode (https://github.com/ComplianceAsCode/content/tree/master/products/sle16/profiles) repository.

TABLE 1: SUPPORTED SCAP SECURITY GUIDE PROFILES FOR SUSE LINUX

Profile name	Profile ID
ANSSI-BP-028 (minimal)	`xccdf_org.ssgproject.content_profile_anssi_bp28_minimal`
ANSSI-BP-028 (intermediary)	`xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary`
ANSSI-BP-028 (enhanced)	`xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced`
ANSSI-BP-028 (high)	`xccdf_org.ssgproject.content_profile_anssi_bp28_high`
Health Insurance Portability and Accountability Act (HIPAA)	`xccdf_org.ssgproject.content_profile_hipaa`
PCI-DSS v4 Control Baseline for SUSE Linux	`xccdf_org.ssgproject.content_profile_pci-dss`

To view the full list of profiles available in the DataStream file, including their IDs, run:

```
> oscap info /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

6 Scanning the system for vulnerabilities

Use **`oscap`** to evaluate your SUSE Linux system against a security profile and generate a report of the results.

6.1 Introduction

The **`oscap xccdf eval`** command evaluates a system against the rules defined in a security profile and produces results in XML format. An HTML report can be generated alongside the XML results for human review. The evaluation typically takes a few minutes, depending on the number of rules in the selected profile.

Before scanning, ensure that the `openscap-utils` and `scap-security-guide` packages are installed as described in *Section 4, "Installing OpenSCAP and the SCAP Security Guide"*, and that you have selected a profile as described in *Section 5, "SSG Content, directories and profiles"*.

6.2 Running a basic scan

To scan your system locally against a profile and save the results, run the following command:

```
> sudo oscap xccdf eval \
  --profile PROFILE-ID \
  --results /tmp/results.xml \
  --report /tmp/report.html \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

Replace *`PROFILE-ID`* with one of the profile IDs listed in *Table 1, "Supported SCAP Security Guide profiles for SUSE Linux"*. For example, to scan against the HIPAA profile:

```
> sudo oscap xccdf eval \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --results /tmp/results.xml \
  --report /tmp/report.html \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

The results are saved to `/tmp/results.xml` and the HTML report to `/tmp/report.html`. Open the report in a web browser to review the evaluation results.

6.3 Using remote resources during a scan

Some SCAP Security Guide content references external OVAL files, for example, to check whether the system is patched against known CVEs. By default, OpenSCAP skips these remote resources and displays a warning. The following options control this behavior.

Fetching remote resources automatically

If the target system has Internet access and you trust the remote content, use the `--fetch-remote-resources` option to download referenced files automatically during the scan:

```
> sudo oscap xccdf eval \
  --fetch-remote-resources \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --results /tmp/results.xml \
```

```
--report /tmp/report.html \
/usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

Using locally downloaded remote resources

On systems without Internet access, or in security-sensitive deployments, download the required remote files in advance and pass them to **oscap** using the `--local-files` option:

1. Create a directory for storing the downloaded files:

```
> mkdir ~/scap-files
```

2. Download the required remote resource:

```
> wget -O ~/scap-files/pub-projects-security-oval-suse.linux.enterprise.15-patch.xml.bz2 \
  https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-patch.xml.bz2
```

Tip

Use the most specific file available for your product version to reduce resource usage and scan time. For example, if you are interested only in a specific service pack, use the corresponding SP-specific file from https://ftp.suse.com/pub/projects/security/oval/.

3. Run the scan using the locally downloaded files:

```
> sudo oscap xccdf eval \
  --local-files ~/scap-files \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --results /tmp/results.xml \
  --report /tmp/report.html \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

4. Optionally, generate an HTML report separately from the XML results file:

```
> oscap xccdf generate report /tmp/results.xml > /tmp/report.html
```

Tip

Separating the scan and the report generation steps reduces resource usage on the target system during the scan itself.

6.4 Scanning with specific rules

By default, **`oscap xccdf eval`** evaluates all rules in the selected profile. You can narrow the scope of evaluation using the following options.

Evaluating a single rule

Use the `--rule` option to evaluate only a specific rule, identified by its rule ID:

```
> sudo oscap xccdf eval \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --rule xccdf_org.ssgproject.content_rule_package_aide_installed \
  --report /tmp/report.html \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

Skipping a specific rule

Use the `--skip-rule` option to exclude a specific rule from the evaluation:

```
> sudo oscap xccdf eval \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --skip-rule xccdf_org.ssgproject.content_rule_package_aide_installed \
  --report /tmp/report.html \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

6.5 Scanning a remote machine

To scan a remote machine over SSH, use **`oscap-ssh`** instead of **`oscap`**. The `openscap-utils` package must be installed on both the local and the remote machine. The interface mirrors that of **`oscap`**:

```
> sudo oscap-ssh user@host 22 xccdf eval \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --results /tmp/results.xml \
  --report /tmp/report.html \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

7 Remediating vulnerabilities

Apply fixes to bring your SUSE Linux system into compliance with a security profile using **`oscap`**, SCAP Security Guide shell scripts, or Ansible playbooks.

7.1 Introduction

After scanning your system, you can remediate identified policy violations automatically or manually. The SCAP Security Guide provides fix scripts in two formats — shell scripts and Ansible playbooks — that **oscap** can apply directly, or that you can review and run independently.

Important: Automatic remediation not always available

Automatic remediation is not offered for fixes that are too disruptive to apply safely on a running system. Such rules must be remediated manually.

The overall remediation process is as follows:

1. **oscap** scans the system and marks each failing rule as a candidate for remediation.
2. For each failing rule, **oscap** locates the corresponding `xccdf:fix` element in the XCCDF file, prepares the environment, and executes the fix script.
3. After executing the fix, **oscap** re-evaluates the rule to confirm whether the fix was successful.
4. All remediation results are stored in an output XCCDF file.

Note

Remediation must be run more than once. Rules are applied in alphabetical order. Some rules have dependencies on others, and the system may need to be restarted between passes for changes to take effect.

7.2 Remediating on the fly

The simplest approach is to scan and remediate in a single command using the `--remediate` option. The system is first scanned, and then **oscap** immediately attempts to fix each failing rule.

Warning: Usage of the `--skip-rule` option

Always use `--skip-rule` to skip the rule `xccdf_org.ssgproject.content_rule_accounts_authorized_local_users` unless you have explicitly configured the variable `var_accounts_authorized_local_users_regex`. Failing to do so may prevent **sudo** from working after a reboot.

```
> sudo oscap xccdf eval --remediate \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --results /tmp/results.xml \
  --report /tmp/report.html \
  --skip-rule xccdf_org.ssgproject.content_rule_accounts_authorized_local_users \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

For the changes to take effect, reboot the system.

```
> sudo reboot
```

In the resulting `/tmp/results.xml` file, the first `TestResult` element contains the scan results before remediation. The second `TestResult` element contains the results after remediation, where a rule result of `fixed` indicates a successful fix, and `error` indicates that the fix was not successful.

7.3 Remediating after scanning

Alternatively, you can separate the scan and remediation into two steps. This allows you to review the scan results before applying any fixes.

1. Scan the system and save the results:

   ```
   > sudo oscap xccdf eval \
     --profile xccdf_org.ssgproject.content_profile_hipaa \
     --results /tmp/results.xml \
     /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
   ```

   The results are stored in a `TestResult` element in `/tmp/results.xml`. The system is evaluated only — no changes are made at this stage.

2. Run remediation using the results file from the previous step as input:

   ```
   > sudo oscap xccdf remediate \
     --results /tmp/results.xml \
     /tmp/results.xml
   ```

   `oscap` creates a new `xccdf:TestResult` element in the same file, inheriting data from the first result and applying fixes only to the rules that failed in the initial scan.

7.4 Generating remediation scripts for review

To inspect the remediation instructions before applying them, use **`oscap xccdf generate fix`** to save the fix content to a file without executing it.

To generate a shell script:

```
> oscap xccdf generate fix \
  --template urn:xccdf:fix:script:sh \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --output my-remediation-script.sh \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

To generate an Ansible playbook:

```
> oscap xccdf generate fix \
  --template urn:xccdf:fix:script:ansible \
  --profile xccdf_org.ssgproject.content_profile_hipaa \
  --output my-remediation-playbook.yml \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

7.5 Remediating with SSG shell scripts

The SCAP Security Guide ships pre-built shell scripts for each supported profile. These can be used for straightforward remediation without conditions or tailoring.

1. List the available shell scripts:

   ```
   > ls -l /usr/share/scap-security-guide/bash/
   ```

   Script names follow the format `sle16-script-PROFILE-NAME.sh`. The supported profile names are: `anssi_bp28_minimal`, `anssi_bp28_intermediary`, `anssi_bp28_enhanced`, `anssi_bp28_high`, `hipaa`, and `pci-dss-4`.

2. Make the script executable:

   ```
   > sudo chmod +x sle16-script-PROFILE-NAME.sh
   ```

3. Run the script:

   ```
   > sudo ./sle16-script-PROFILE-NAME.sh
   ```

Note

Within each script, rules follow the format: `# BEGIN fix (N/TOTAL) for RULE-ID` through to `# END fix for RULE-ID`. Rules that contain a line ending with `IS MISSING!` have no automatic remediation and must be applied manually.

7.6 Remediating with Ansible playbooks

For each supported profile, the SCAP Security Guide also ships Ansible playbooks that you can use for remediation.

1. Install the `ansible` package.

```
> sudo zypper install ansible
```

2. List the available Ansible playbooks:

```
> ls -l /usr/share/scap-security-guide/ansible/
```

   Playbook names follow the format `sle16-playbook-PROFILE-NAME.yml`.

3. Create an inventory file `ansible_inventory.yml` with the following content:

```
all:
  hosts:
    localhost
  vars:
    ansible_connection: local
```

4. Run the playbook:

```
> sudo ansible-playbook -i ansible_inventory.yml \
  sle16-playbook-PROFILE-NAME.yml
```

5. To skip specific rules during execution, use the `--tags` option. Find the tag for a rule by searching for it in the playbook file. For example:

```
> sudo ansible-playbook -i ansible_inventory.yml \
  sle16-playbook-PROFILE-NAME.yml \
  --tags "package_aide_installed,aide_build_database"
```

Note

You may need to repeat the remediation steps more than once. Some rules require a system restart to take effect, and rules are executed in alphabetical order, which means dependencies between rules may not be resolved in a single pass.

7.7 Customizing the SCAP Security Guide with SCAP Workbench

If the available profiles do not fully match your requirements, you can create a customized profile using SCAP Workbench and save it as a tailoring file. The tailoring file can then be applied with **oscap** using the `--tailoring-file` option.

1. Start SCAP Workbench:

```
> sudo scap-workbench
```

2. Select `SLE16` as the target system variant, then select *Load Content*.
3. Select a base profile from the *Profile* drop-down list, then select *Customize*.
4. Set a unique ID for the custom profile in the following format: `xccdf_`*`REVERSE-DNS`*`_profile_`*`PROFILE-NAME`*. For example: `xccdf_org.`*`mycompany`*`_profile_`*`server`*.

Warning

The profile ID cannot be changed after it is set in SCAP Workbench.

5. Deselect any rules you do not want to include, then select *OK*.
6. Save the customization as a tailoring file: select *Select customization file* > *Open* > *Save customization only*.
7. Apply the tailoring file with **oscap**:

```
> sudo oscap xccdf eval \
  --profile xccdf_org.mycompany_profile_server \
  --tailoring-file ssg-sle16-ds-tailoring.xml \
  --report /tmp/report.html \
  /usr/share/xml/scap/ssg/content/ssg-sle16-ds.xml
```

8 For more information

- The OpenSCAP project and documentation: https://www.open-scap.org/security-policies/scap-security-guide/
- The OpenSCAP User Manual: https://static.open-scap.org/openscap-1.2/oscap_user_manual.html

- The `SCAP Security Guide` upstream repository and README: https://github.com/ComplianceAsCode/content/
- Online profile guides for all products: https://complianceascode.github.io/content-pages/guides/index.html
- OVAL security data provided by SUSE: https://www.suse.com/support/security/oval/

9 What's next

After hardening your system, consider the following steps to maintain and improve your security posture:

- Schedule regular scans to detect configuration drift and verify that the system remains compliant after updates or changes.
- Use the test environment established during infrastructure preparation to validate new versions of the SCAP Security Guide before applying them to production.
- Review and document any rules that could not be remediated automatically, and ensure compensating controls are in place for each.
- Consider integrating OpenSCAP scanning into your CI/CD or configuration management pipeline for continuous compliance monitoring.
- Keep the `scap-security-guide` package up to date to benefit from the latest security rules and profile improvements.

10 Legal Notice

Copyright© 2006– 2026 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled “GNU Free Documentation License”.

For SUSE trademarks, see https://www.suse.com/company/legal/. All other third-party trademarks are the property of their respective owners. Trademark symbols (®, ™ etc.) denote trademarks of SUSE and its affiliates. Asterisks (*) denote third-party trademarks.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

A GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download

using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been

published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.