OPEN SOURCE SOFTWARE

SECURITY & MAINTENANCE GUIDE

A Practical Guide for Canadian Organizations

Linux Association of Canada
linuxassociation.ca

Contents

Note: This excerpt begins with the Weekly Tasks section of the full maintenance checklist. Daily tasks and earlier chapters are covered in preceding pages of the complete guide.

MAINTENANCE CHECKLIST

Keeping Your Systems Secure

Weekly, Monthly, Quarterly & Annual Tasks

Maintenance Checklist

A consistent maintenance routine is the foundation of a secure technology environment. The following checklist outlines recommended tasks organized by frequency, along with estimated time requirements and suggested responsibility.

Weekly Tasks

☐ Review Security Advisories

- Your Linux distribution's security mailing list
- Security advisories for critical applications
- Canadian Centre for Cyber Security alerts
- CISA Known Exploited Vulnerabilities catalog

Time required: 15-30 minutes
Responsibility: IT staff or security coordinator

☐ Review Pending Updates

- Identify security updates requiring immediate attention
- Note feature updates for scheduled maintenance
- Prioritize based on severity and system exposure
- Document any updates requiring special testing

Time required: 15-20 minutes
Responsibility: IT staff

☐ Review System Logs

- Failed login attempts
- Service errors or crashes
- Unusual network connections
- Disk space warnings

Time required: 10-15 minutes
Responsibility: IT staff

Monthly Tasks

☐ Install Security Updates

- Review all pending security updates

- Test updates in development environment if possible
- Install updates on production systems
- Verify services restart correctly
- Monitor system logs after updates
- Document what was updated and when

Time required: 1-3 hours depending on number of systems
Responsibility: IT staff with management notification

☐ Verify Backup Completion

- Review backup logs for successful completion
- Verify backup file sizes are reasonable
- Confirm backup storage has adequate capacity
- Check that backup retention policies are being followed
- Test restoration of at least one file or database

Time required: 30-45 minutes
Responsibility: IT staff or backup administrator

☐ Review User Accounts

- Review list of active user accounts
- Disable accounts for departed staff
- Verify that user permissions are appropriate
- Check for any suspicious account activity
- Remove temporary accounts that are no longer needed

Time required: 20-30 minutes
Responsibility: IT staff with HR coordination

☐ Update Software Inventory

- Document any newly installed software
- Update version numbers for updated software
- Note any software that was removed
- Verify support status hasn't changed

Time required: 15-20 minutes
Responsibility: IT staff

Quarterly Tasks

☐ Remove Unused Software

- Review all installed applications and services
- Identify software that is no longer actively used
- Remove unnecessary software and services
- Document what was removed and why
- Verify that removal didn't affect other systems

Time required: 1-2 hours
Responsibility: IT staff with user consultation

☐ Test Firewall Configuration

- Review current firewall rules
- Confirm only necessary ports are open
- Test that unauthorized access is blocked
- Document any configuration changes
- Verify logging is functioning

Time required: 1-2 hours
Responsibility: IT staff or network administrator

☐ Verify Disaster Recovery Procedures

- Review disaster recovery documentation
- Verify that recovery procedures are current
- Test restoration from backups
- Update contact information for emergency response
- Conduct tabletop exercise if possible

Time required: 2-4 hours
Responsibility: IT staff with management participation

☐ Review Security Policies

- Review security policies and procedures
- Update based on lessons learned
- Ensure policies reflect current systems and services
- Communicate any policy changes to staff

Time required: 1-2 hours
Responsibility: IT staff with management review

Annual Tasks

☐ Comprehensive Software Inventory Review

- Document all software in use across organization
- Record current versions and installation dates
- Verify support status and End of Life dates
- Identify software approaching EOL
- Plan upgrades for unsupported or soon-to-be-unsupported software

Time required: 4-8 hours depending on organization size
Responsibility: IT staff with management review

☐ Upgrade Unsupported Systems

- Prioritize systems running unsupported software
- Plan and test major upgrades
- Schedule extended maintenance windows
- Communicate planned downtime to users
- Verify successful completion and functionality

Time required: Variable, often requires multiple days
Responsibility: IT staff with management approval

☐ Update Security Policies and Procedures

- Review all security policies and procedures
- Update based on changes in technology environment
- Incorporate lessons learned from incidents
- Ensure staff are aware of current policies
- Obtain management approval for policy changes

Time required: 4-6 hours
Responsibility: IT staff with management and legal review

☐ Review and Test Incident Response Plan

- Review incident response procedures
- Update contact information for all stakeholders
- Conduct tabletop exercise simulating security incident
- Document improvements to procedures
- Train staff on their roles in incident response

Time required: 4-6 hours

Responsibility: IT staff with management participation

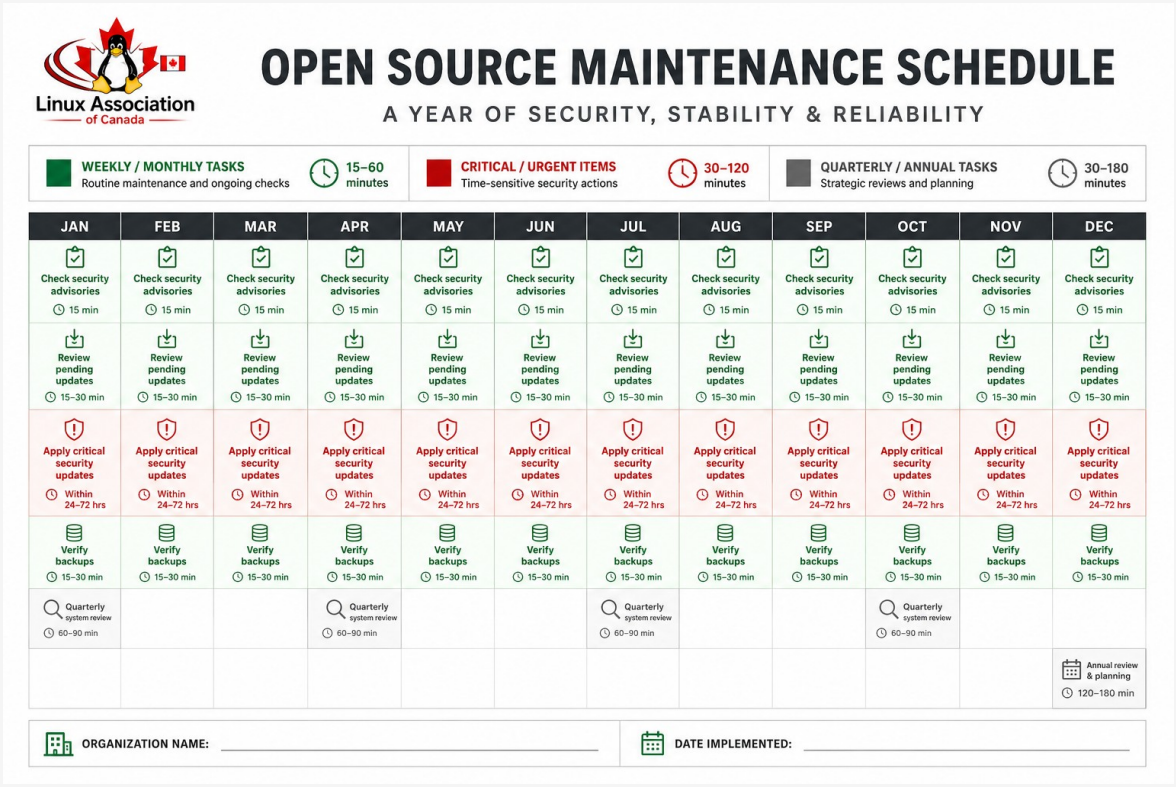
☐ Security Training and Awareness

- Conduct security awareness training for all staff
- Cover password security, phishing recognition, and safe computing
- Provide role-specific training for IT staff
- Document training completion
- Update training materials based on current threats

Time required: 2-4 hours per staff member
Responsibility: IT staff or external security trainer

Notes on Using This Checklist

- Adapt to your environment – Not all tasks will apply to every organization. Modify this checklist to reflect your specific systems and needs.
- Document completion – Keep records of when tasks were completed and by whom. This documentation demonstrates due diligence and helps identify patterns.
- Start gradually – If you're not currently following any maintenance routine, begin with the most critical tasks and add others over time.
- Assign responsibility – Clearly designate who is responsible for each task. In small organizations, one person may handle everything, but responsibility should still be explicit.
- Schedule reminders – Use calendar reminders or task management systems to ensure routine tasks aren't forgotten.
- Review and improve – Periodically review whether your maintenance routine is working effectively and adjust as needed.



Linux Association of Canada

OPEN SOURCE MAINTENANCE SCHEDULE

A YEAR OF SECURITY, STABILITY & RELIABILITY

WEEKLY / MONTHLY TASKS Routine maintenance and ongoing checks	15–60 minutes	**CRITICAL / URGENT ITEMS** Time-sensitive security actions	30–120 minutes
QUARTERLY / ANNUAL TASKS Strategic reviews and planning	30–180 minutes		

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min	Check security advisories 15 min
Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min	Review pending updates 15–30 min
Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs	Apply critical security updates Within 24–72 hrs
Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min	Verify backups 15–30 min
Quarterly system review 60–90 min			Quarterly system review 60–90 min			Quarterly system review 60–90 min			Quarterly system review 60–90 min		
											Annual review & planning 120–180 min

ORGANIZATION NAME: _____ **DATE IMPLEMENTED:** _____

RESOURCES

Where to Learn More

Authoritative sources for open source security guidance

Where to Learn More

Maintaining awareness of security developments and best practices requires access to reliable information sources. The following resources provide authoritative guidance on open source security, vulnerability management, and cybersecurity best practices.

Canadian Centre for Cyber Security

Website: cyber.gc.ca

The Canadian Centre for Cyber Security is Canada's national authority on cybersecurity. They provide:

- Alerts and advisories on current cyber threats affecting Canadian organizations
- Best practice guidance for organizations of all sizes
- Cyber security publications including implementation guides
- Incident reporting resources for Canadian organizations
- Baseline security controls for IT systems

Recommended resources:

- ITSG-33: IT Security Risk Management
- Cyber security best practices for small and medium organizations
- Ransomware playbook
- Security considerations for cloud computing

CISA (Cybersecurity and Infrastructure Security Agency)

Website: cisa.gov

CISA is the United States' cybersecurity agency, providing valuable resources applicable to organizations worldwide:

- Known Exploited Vulnerabilities Catalog – Actively exploited vulnerabilities requiring immediate attention
- Security advisories on critical infrastructure threats
- Free cybersecurity services including vulnerability scanning
- Cybersecurity best practices and implementation guides
- Incident response resources

Recommended resources:

- Known Exploited Vulnerabilities (KEV) catalog
- Cybersecurity Performance Goals for critical infrastructure
- Free cybersecurity services for organizations
- Shields Up awareness campaign

CVE Program and National Vulnerability Database

Website: cve.org • nvd.nist.gov

These complementary resources provide comprehensive vulnerability information.

- CVE: standardized identifiers for publicly known vulnerabilities, brief descriptions, and references to additional information sources
- NVD: enhanced CVE information with severity scores, detailed technical analysis, affected software versions, available patches and workarounds, and a searchable database of all known vulnerabilities

Linux Distribution Security Resources

Each major Linux distribution maintains dedicated security resources:

- Ubuntu Security — ubuntu.com/security — Ubuntu Security Notices (USN), CVE tracking, security update procedures
- Red Hat / CentOS / Fedora Security — access.redhat.com/security — Red Hat Security Advisories (RHSA), updates and errata
- Debian Security — debian.org/security — Debian Security Advisories (DSA), security tracker
- SUSE Security — suse.com/security — SUSE Security Announcements, updates and patches

Subscribe to security mailing lists for your specific Linux distribution to receive timely notifications of security updates.

Software Project Security Resources

Individual open source projects maintain their own security resources, typically including security policies and responsible disclosure procedures, security advisories, mailing lists, and contact information for reporting vulnerabilities.

- WordPress — wordpress.org/news/category/security
- Apache — apache.org/security
- PostgreSQL — postgresql.org/support/security
- Docker — docs.docker.com/engine/security
- Kubernetes — kubernetes.io/docs/concepts/security

For any critical software your organization uses, bookmark the project's security page and subscribe to security announcements.

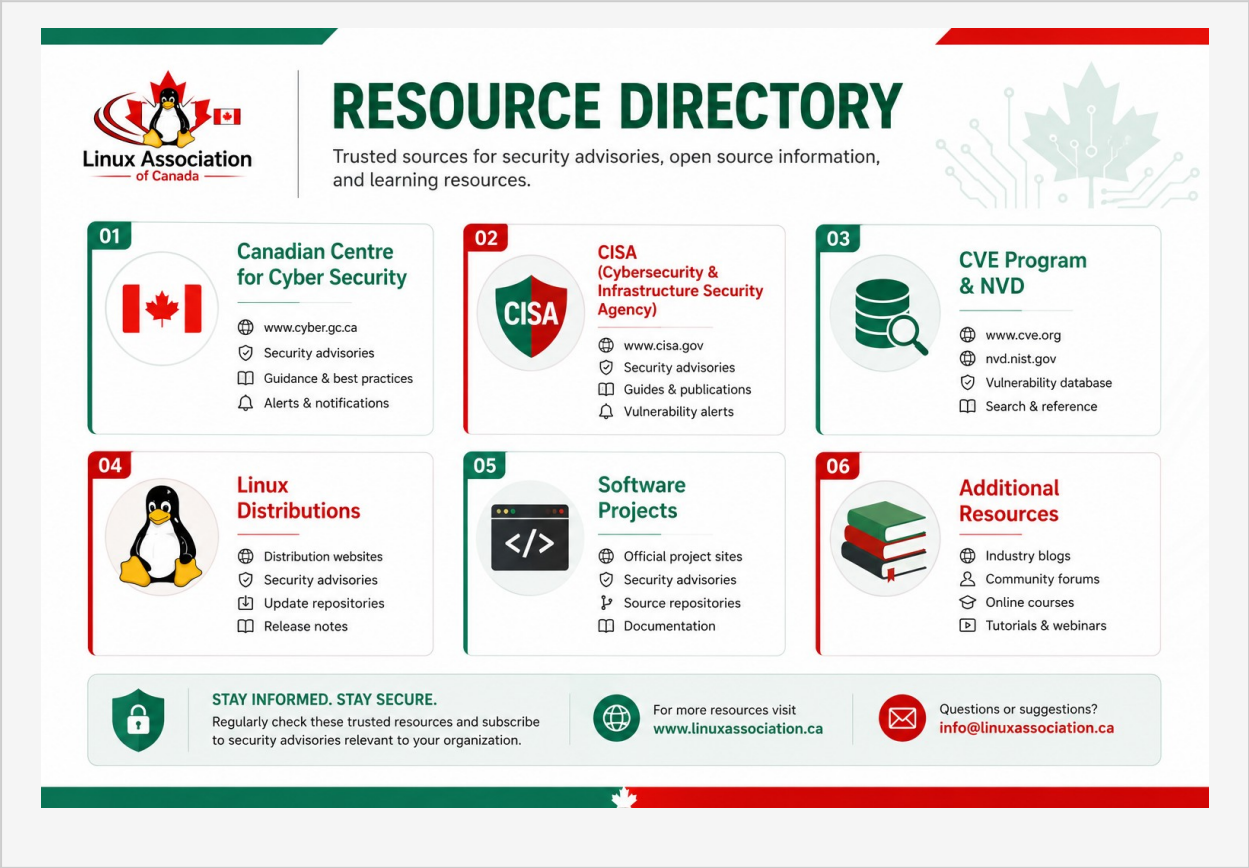
Additional Learning Resources

- SANS Institute — sans.org — cybersecurity training and certification, free resources, Internet Storm Center
- OWASP — owasp.org — web application security guidance, Top 10 risks, free tools and documentation
- Linux Foundation — linuxfoundation.org — open source security initiatives, training and certification

Staying Informed

Establish a routine for monitoring security information:

- Subscribe to relevant mailing lists – security announcements from your Linux distribution and critical applications
- Set up RSS feeds or alerts – for security news sources relevant to your technology stack
- Dedicate time weekly – spend 15-30 minutes reviewing security advisories
- Share information – ensure relevant security information reaches decision-makers
- Participate in communities – join local Linux user groups or online communities



REFLECTIONS

Final Thoughts

Security as an ongoing process, not a destination

Final Thoughts

Open source software represents one of humanity's most successful collaborative endeavors. From the servers powering the Internet to the smartphones in our pockets, from municipal services to healthcare systems, open source technology enables the digital infrastructure that modern society depends upon.

This collaborative model provides significant advantages: flexibility to adapt software to specific needs, transparency that enables security verification, innovation driven by diverse global contributors, and long-term sustainability that doesn't depend on any single vendor's business decisions.

However, like every technology—whether open source or proprietary, simple or complex, free or commercial—software requires regular care and maintenance to remain secure.

The Reality of Software Security

No software is perfect. Vulnerabilities are discovered in all software products, and this is completely normal. What distinguishes secure organizations from vulnerable ones is not the absence of vulnerabilities in their software, but rather their ability to respond quickly when vulnerabilities are identified.

The most significant cybersecurity risk facing organizations today is not sophisticated zero-day exploits or advanced persistent threats. The most significant risk is running outdated software with known vulnerabilities that have already been fixed.

Organizations that establish simple, consistent maintenance routines dramatically reduce their cybersecurity risk while benefiting from one of the world's most collaborative and innovative technology ecosystems.

Security as Process, Not Product

Security is not something you purchase and install. Security is not achieved through a single action or decision. Security is an ongoing process built through:

- Awareness – Understanding the technology you use, where it comes from, and how it's maintained
- Maintenance – Establishing consistent routines for reviewing advisories, installing updates, and verifying system health
- Preparation – Maintaining backups, documenting procedures, and preparing for potential incidents
- Responsibility – Assigning clear ownership for security tasks and ensuring they're completed consistently
- Improvement – Learning from experience and continuously refining your security practices

Organizations that embrace security as an ongoing process rather than a one-time project build

resilient, sustainable technology environments.

Starting Your Journey

If your organization is not currently following consistent maintenance routines, the prospect of implementing everything described in this guide may seem overwhelming. Remember that security improvement is a journey, not a destination.

Start with the highest-impact practices:

- Enable automatic security updates where possible
- Establish regular backup verification
- Subscribe to security advisories for your critical systems
- Remove unused software
- Document what software you're running

Then gradually expand your practices:

- Implement a monthly maintenance window
- Conduct quarterly security audits
- Develop incident response procedures
- Provide security awareness training
- Continuously refine and improve

Every step forward improves your security posture. Progress matters more than perfection.

The Broader Context

The security practices described in this guide extend beyond just open source software. The principles of regular maintenance, timely updates, backup verification, and consistent routines apply equally to proprietary software, cloud services, and all technology systems.

Open source software, with its transparency and collaborative development model, often makes these security practices easier to implement. Public vulnerability databases, active security communities, and rapid patch development mean that organizations using open source software can often respond to security issues more quickly than those dependent on proprietary vendors.

Building a Security Culture

Technology security ultimately depends on people. The most sophisticated security tools and procedures are ineffective if staff don't understand their importance or don't follow them consistently.

Building a security culture means:

- Making security everyone's responsibility, not just the IT department's concern
- Providing clear, understandable guidance rather than complex technical jargon
- Recognizing and rewarding good security practices rather than only responding to problems

- Learning from incidents without blame, focusing on improvement
- Communicating openly about security challenges and successes

Organizations with strong security cultures naturally maintain better security practices because staff understand why security matters and how their actions contribute to organizational safety.

Looking Forward

The technology landscape continues to evolve. New software, new threats, and new best practices emerge constantly. Organizations that establish strong foundational security practices—regular maintenance, consistent monitoring, verified backups, and documented procedures—can adapt to these changes effectively.

The Linux Association of Canada remains committed to helping Canadian organizations, communities, educational institutions, and individuals navigate the open source ecosystem successfully. We believe that open source software, maintained responsibly, provides Canadian organizations with secure, sustainable, and sovereign technology solutions.

Your Next Steps

After reading this guide:

- Assess your current practices – How do your current maintenance routines compare to the recommendations in this guide?
- Identify gaps – What critical practices are you not currently following?
- Prioritize improvements – Which changes would have the greatest security impact?
- Create an action plan – What specific steps will you take, and when?
- Assign responsibility – Who will ensure these improvements are implemented?
- Start today – Begin with one small improvement rather than waiting for the perfect comprehensive plan.

Security improvement begins with a single step. Take that step today.

In Closing

Open source software has transformed the world, enabling innovation, collaboration, and technological advancement on an unprecedented scale. By combining the power of open source technology with consistent, responsible maintenance practices, organizations of all sizes can build secure, sustainable digital infrastructure.

Security is not about eliminating all risk—that's impossible. Security is about making informed decisions, implementing reasonable safeguards, and maintaining consistent practices that significantly reduce risk to acceptable levels.

The practices described in this guide are achievable for organizations of all sizes. They don't require expensive security products, large IT departments, or specialized expertise. They require commitment, consistency, and a recognition that security is an ongoing process, not a destination.

Thank you for taking the time to read this guide. We hope it helps your organization build more

secure, sustainable technology practices.

OUR ORGANIZATION

About the Linux Association of Canada

Advancing open source, digital sovereignty & education

About the Linux Association of Canada

The Linux Association of Canada is a national non-profit organization dedicated to advancing Linux, open source software, digital sovereignty, and technology education across Canada.

Our Mission

We exist to help Canadians—individuals, organizations, educational institutions, businesses, and governments—make informed decisions about adopting and maintaining secure, sustainable open source technologies.

We believe that open source software provides Canadian organizations with:

- Digital sovereignty – Control over technology infrastructure without dependence on foreign vendors
- Transparency – Ability to verify security and functionality
- Flexibility – Freedom to adapt software to Canadian needs
- Sustainability – Long-term viability independent of any single company
- Innovation – Access to cutting-edge technology developed by global communities
- Cost effectiveness – Reduced licensing costs and vendor lock-in

What We Do

Educational Publications

We create accessible, practical guides that help Canadians understand and effectively use open source technology, translating complex technical concepts into clear, actionable guidance.

Community Outreach

We connect with communities across Canada to raise awareness about open source software, its benefits, and best practices for implementation and maintenance.

Linux User Group Support

We support local Linux user groups across Canada, providing resources, coordination, and national networking opportunities.

Open Source Awareness

We work to increase understanding of open source software among Canadian organizations, dispelling misconceptions and highlighting security, flexibility, and sustainability advantages.

Digital Sovereignty Initiatives

We advocate for Canadian control over critical digital infrastructure through open source adoption.

Best Practice Guidance

We develop and share best practices for open source deployment, security maintenance, and lifecycle management, tailored for Canadian organizations.

Public Resources

We maintain freely available guides, checklists, documentation, and reference materials to help Canadians succeed with open source technology.

National Collaboration

We facilitate connections between Canadian organizations, educational institutions, government agencies, and open source communities.

Who We Serve

Small and Medium Organizations

We help businesses, non-profits, and community organizations implement secure, cost-effective open source solutions appropriate for their needs and resources.

Educational Institutions

We support schools, colleges, and universities in adopting open source technology for teaching, learning, and administration, preparing students for technology careers.

Municipal and Regional Governments

We assist local governments in evaluating and implementing open source solutions for public services, reducing costs while maintaining control over critical infrastructure.

Community Groups

We work with community organizations, libraries, and citizen groups to increase access to technology through open source solutions.

IT Professionals

We provide resources and networking opportunities for IT professionals working with or interested in open source technology.

Individuals

We help individual Canadians learn about and adopt open source software for personal and professional use.

Our Approach

Practical, Not Ideological

While we're passionate about open source software, we recognize that technology decisions must be practical. We provide balanced guidance acknowledging both strengths and limitations.

Accessible, Not Technical

We translate complex technical concepts into clear language that decision-makers, community members, and non-technical stakeholders can understand and act upon.

Canadian Context

We understand Canadian regulatory requirements, privacy laws, bilingual needs, and the unique challenges facing Canadian organizations.

Evidence-Based

Our recommendations are based on established best practices, security research, and real-world experience, not vendor marketing or unsubstantiated claims.

Inclusive and Collaborative

We believe technology should be accessible to all Canadians, and work to ensure open source adoption is inclusive, considering diverse needs, languages, and accessibility requirements.

Our Values

Transparency

We operate openly, sharing our knowledge, resources, and processes with the Canadian community.

Collaboration

We believe that working together—across organizations, sectors, and communities—produces better outcomes than working in isolation.

Education

We're committed to helping Canadians understand technology, make informed decisions, and build sustainable digital infrastructure.

Sovereignty

We believe Canadians should control their digital infrastructure and not be dependent on foreign technology vendors for critical systems.

Sustainability

We promote technology solutions that are sustainable long-term, both economically and environmentally.

Accessibility

We work to ensure that technology benefits all Canadians, regardless of resources, location, or technical expertise.

Get Involved

For Organizations:

- Adopt open source solutions with our guidance
- Share your experiences with other Canadian organizations
- Participate in our educational initiatives
- Support open source adoption in your sector

For Individuals:

- Join or start a local Linux user group
- Contribute to open source projects
- Share knowledge with your community
- Advocate for open source adoption

For IT Professionals:

- Connect with peers across Canada
- Share best practices and lessons learned
- Contribute to our educational resources
- Mentor others in open source technology

For Educators:

- Integrate open source into curriculum
- Prepare students for technology careers
- Connect with other educational institutions
- Access our educational resources

Our Commitment

Whether you're taking your first steps with open source software or managing a complex open source infrastructure, the Linux Association of Canada is committed to supporting your success.

We provide the guidance, resources, and community connections you need to implement secure, sustainable open source solutions that serve Canadian needs.

Together, we're building a more secure, sovereign, and sustainable digital future for Canada.


Linux Association of Canada
OPEN SOURCE.
STRONG COMMUNITIES.
BETTER CANADA.
Connecting people, technology and communities from coast to coast to coast.
LEARNING LINUX
BUILDING STRONGER COMMUNITIES TOGETHER
LOCAL COMMUNITY OPEN SOURCE BIG IMPACT
DISCOVER
LEARN
SHARE
OPEN SOURCE
TOGETHER WE BUILD A BETTER DIGITAL CANADA
VOLUNTEER
SECURE. RELIABLE. OPEN SOURCE.
BETTER CARE FOR CANADIANS.
COLLABORATION
INNOVATION
EDUCATION
ACCESSIBILITY
SOVEREIGNTY
COMMUNITY
OPEN SOURCE IS MORE THAN CODE. IT'S PEOPLE. COLLABORATION. AND A STRONGER CANADA FOR EVERYONE.

Contact Us

Website

linuxassociation.ca
Additional guides, news, community connections, educational materials, and event information.

Email

info@linuxassociation.ca
Questions about open source adoption, security guidance, speaking engagements, partnerships, and general inquiries.

Phone

(639) 477-0111
Consultation requests, media inquiries, organizational support, and community connections.

Connect With Us

Mastodon: @linuxassociation@thecanadian.social
Bluesky: @linuxassociation.ca
LinkedIn: Linux Association of Canada

Join the Conversation

- Connect with local Linux user groups
- Participate in open source projects
- Share your experiences and knowledge

- Support open source adoption in your community
- Advocate for digital sovereignty

Acknowledgments

This guide was developed with input from Canadian IT professionals, security researchers, open source contributors, and community members across the country. We're grateful for their expertise and commitment to helping Canadian organizations adopt secure, sustainable technology solutions.

Published 2026 • Linux Association of Canada

Building a more secure, sovereign, and sustainable digital future for Canada