PRIXL

FREE TEMPLATE · ADOPT, ADAPT AND SHARE

Information Security Policy for CA Firms

A practical framework for chartered accountant firms and professional practices

Version 3.1 · October 2026 · Prixl Technologies

HOW TO USE THIS DOCUMENT

This is a suggested framework, not a mandatory standard. Your technology, staff size, clients and appetite for risk decide which controls fit your firm. It is general information, not legal advice, and adopting it does not by itself make a firm compliant with any law. Review it with your partners, your IT advisor and, for the legal duties, a legal advisor. Adopt the controls that apply, adjust the ones that need it, and write down why you left any out. A short policy your team follows is worth more than a long one that sits in a drawer. Once it is final, every person in the firm should read it and know their part in it.

Purpose. This document gives chartered accountant firms and similar practices a practical information security policy to adopt, adapt and review every year. It aims to be practical and honest, so it covers controls that no single product provides. Prixl Technologies makes Prixl Warden: the closing section says where our product fits and where it does not, and every control here applies whatever tools you use.

Adopted by (firm) _____ Date adopted _____

Security Officer _____ Next review due _____

Regulatory obligations

These laws put duties on CA firms in India for information security, data protection and incident reporting. This is a summary for awareness. Laws change, so confirm what applies to your firm with a legal advisor.

Law or rule	Status	Who it applies to	What it requires	Consequence
IT Act 2000, Section 43A, and the SPDI Rules 2011	In force	Every body corporate, which for Section 43A includes a firm or sole proprietorship in professional activities, that handles sensitive personal data such as passwords (including clients' tax and GST portal passwords) and bank account or card details.	Reasonable security practices, with a documented information security programme and policy. A firm relying on ISO 27001 or another approved code is deemed compliant only if an independent auditor approved by the Central Government audits it at least once a year and after significant changes. A privacy policy published on the firm's website. Written consent before collecting sensitive data, and use only for that purpose. A Grievance Officer whose contact details are published.	Compensation to affected persons under Section 43A. A penalty of up to ₹25 lakh under Section 72A for disclosing personal information without consent or in breach of a lawful contract, with intent to cause wrongful loss or gain.
CERT-In Directions of 28 April 2022 (Section 70B(6), IT Act), effective 27 June 2022, or 25 September 2022 for MSMEs	In force	Service providers, intermediaries, data centres, body corporates and government organisations. CERT-In's FAQ treats a firm as a body corporate.	Report specified cyber incidents to CERT-In within 6 hours of noticing them or being told of them. Keep logs of all ICT systems for a rolling 180 days, within India. Synchronise system clocks with NIC or NPL time servers. Name a point of contact and send their details to CERT-In.	Imprisonment up to 1 year, or a fine up to ₹1 crore, or both (Section 70B(7), as amended from 30 November 2023).
Chartered Accountants Act 1949, Second Schedule, Part I, Clause (1), and the ICAI Code of Ethics (2026 edition)	In force	Members in practice. Members in employment have a similar duty under Part II, Clause (2).	Do not disclose information gained in a professional engagement without the client's consent or a legal requirement. The duty continues after the engagement ends and covers all information gained in the engagement.	Professional misconduct: reprimand, removal of the member's name from the register for a period or permanently, or a fine of up to ₹5 lakh (Section 21B).

Law or rule	Status	Who it applies to	What it requires	Consequence
Digital Personal Data Protection Act 2023 and DPDP Rules 2025	Phased. Rules notified 13 November 2025; the main duties apply from May 2027.	Data fiduciaries: anyone who decides why and how digital personal data is processed. A CA firm is one for most of the personal data it holds about clients and staff; where it only processes data on a client's behalf, such as running the client's payroll, it may be a data processor instead.	Reasonable security safeguards, including keeping logs for at least one year. Tell the Data Protection Board and each affected person of any personal data breach without delay, with a detailed report to the Board within 72 hours. A published contact for questions about personal data, and a way to handle complaints. Honour rights to access, correct and erase. A Data Protection Officer for significant data fiduciaries.	Penalties up to ₹250 crore for failing to take reasonable security safeguards, and up to ₹200 crore for failing to report a breach. Section 43A of the IT Act, the basis of the SPDI Rules, is omitted on the same date (DPDP Act, section 44(2)).
Companies Act 2013, Section 128	In force for companies	Your client companies, whose books you may hold or process. CA firms cannot practise as companies (CA Act, section 25); a CA firm that is an LLP keeps its books under the LLP Act for eight years.	Books of account kept for at least 8 financial years. Electronic books allowed, with a daily back-up on a server in India.	Fine of ₹50,000 to ₹5,00,000 on the officers responsible. The imprisonment clause was removed in December 2020.

ACT NOW: CERT-IN 2022

Many small firms are not yet set up for these directions. Three steps:

1. Name a point of contact and send their details to info@cert-in.org.in. Note CERT-In's reporting contacts: email incident@cert-in.org.in, toll-free phone 1800-11-4949, fax 1800-11-6969.
2. Keep the logs of every server for 180 days, as the directions require. We recommend the full Windows Security, System and Application logs, with failed as well as successful events: archive the complete log files, not only alerts. Ask your IT provider to set up a daily compressed export to separate storage in India. From May 2027 the DPDP Rules require logs to be kept for at least one year.
3. Set server clocks to the NIC time servers samay1.nic.in and samay2.nic.in, or NPL's time.nplindia.org, with Windows Date & Time settings or the `w32tm` command.

The 6-hour reporting clock already applies. Ransomware, unauthorised access to a server and a data breach all count.

GET READY: DPDP ACT, MAY 2027

The DPDP Act will ask firms to formalise how they handle personal data. A firm that runs this policy, together with sound backup and retention practice, will have most of the security groundwork in place. Before May 2027, add: a record of what personal data you hold and why; a privacy notice and consent process where consent is your basis for using the data (staff records and some client data can rest on other lawful grounds); a named contact for questions and complaints about personal data; a breach notification procedure; and one-year log retention. Check the current commencement date before relying on it.

Other points.

- **Client confidentiality.** Tell clients how you protect their data in your engagement letter.
- **Clients abroad.** If you serve clients in the EU or handle data of people there, the GDPR may apply. Take advice.
- **Retention periods.** Audit documentation is ordinarily kept for at least seven years from the date of the auditor's report (SA 230 and SQC 1). Books under the Income-tax Act 2025 are kept for seven tax years from the end of the relevant tax year (rule 46 of the Income-tax Rules 2026). GST records are kept for 72 months from the due date of the annual return, or longer while an appeal or investigation is pending. Confirm the periods that apply to each kind of record with your advisor.

1. Governance and accountability

Security without an owner fails. Assign responsibility before any technical control.

Action	Why it matters	Priority	Frequency
Appoint one person as Security Officer	One named person owns security decisions, incident response and policy reviews. They do not need to be technical; they need to be careful and available.	**High**	Once; reviewed every year
Keep a Security Register	A simple log of incidents, policy changes and audit findings, kept as evidence of due care. A shared spreadsheet is enough.	**High**	Ongoing
Run a quarterly internal security review	Check access lists, open incidents, backups and the server's security settings. It takes one to two hours a quarter.	**High**	Quarterly
Have an independent annual security audit	Your own team has blind spots. An outside consultant reviews servers, access, backups and policy compliance and gives a written report. It is a condition of relying on ISO 27001 under the SPDI Rules, and the report is evidence of due care if a client or ICAI asks after an incident.	**High**	Every year
Keep an asset register	List every device that can reach client data: servers, laptops and phones. You cannot protect data until you know where it lives.	**Medium**	When devices change
Classify your data	Public, internal and confidential. Client financial data is confidential and gets the strictest controls.	**Medium**	Once; reviewed every year

2. Server and system security

The Windows server is the most important asset in the firm. Remote Desktop exposed to the internet and unpatched software are among the most common ways into it.

Action	Why it matters	Priority	Frequency
Install Windows security updates within 30 days, critical ones within 7	In Sophos's 2025 survey, unpatched software was the most common way ransomware got in. Microsoft publishes fixes on the second Tuesday of each month.	**High**	Monthly
Keep Microsoft Defender or another antivirus running and up to date	Real-time protection stops known malware before it runs. If you use a third-party product, check that it is active.	**High**	Always on; checked quarterly
Keep Windows Firewall on for all three profiles	Domain, private and public profiles should all be on. A profile switched off, often by remote-support or other software, leaves every listening service reachable from any network that uses that profile.	**High**	Always on; checked monthly

Action	Why it matters	Priority	Frequency
Disable SMBv1	The protocol behind WannaCry. A modern Windows server has no use for it.	**High**	Once
Require Network Level Authentication for Remote Desktop	Users must authenticate before a session starts, which blocks a class of pre-login attacks.	**High**	Once
Disable the built-in Guest account	It allows limited access without a password.	**High**	Once
Keep administrator accounts to a minimum	Give each person who needs admin rights a named account. Rename or disable the built-in Administrator and give it a long random password kept in a safe place. Remove admin rights the day someone no longer needs them.	**High**	Reviewed quarterly
Turn on PowerShell script block logging	Records the PowerShell code run on the server, including code an attacker unpacks at run time, for investigation after an incident.	**Medium**	Once
Disable services you do not use	IIS, FTP and Telnet are common examples. Every running service is something to attack. Check with your IT provider before disabling Remote Registry: some monitoring and backup tools need it.	**Medium**	Once; reviewed every year
Review the server's security log every month	Sign-ins, failures, account changes and policy changes are all recorded. Ten minutes a month catches unusual patterns.	**Medium**	Monthly

3. Access control and passwords

Weak passwords and too much access cause most account takeovers. This section follows NIST's 2025 guidance (SP 800-63B-4), which favours long passphrases over complexity rules and forced changes.

Action	Why it matters	Priority	Frequency
Require passwords of at least 15 characters, and encourage passphrases	Length is what makes a password hard to guess. NIST sets 15 characters as the minimum for a password used without a second factor. Four or five unrelated words are easy to remember and hard to crack. Windows enforces more than 14 only after "Relax minimum password length limits" is turned on, on Windows Server 2022 and later; test it first, as some older software may not cope. On older servers set 14, the most they allow.	**High**	Set once
Lock an account after 5 to 10 failed attempts, for at least 15 minutes	Stops password guessing against a single account. CIS suggests 5 and Microsoft's baseline 10. With Remote Desktop open to the internet, attackers can use lockout to keep real users out: one more reason to close it. On servers set up before October 2022, also turn on "Allow Administrator account lockout", or the built-in Administrator is never locked.	**High**	Set once

Action	Why it matters	Priority	Frequency
Remember the last 24 passwords, with a minimum password age of 1 day	Stops people cycling back to an old password. Without a minimum age, someone can change it 24 times in a row and get the old one back.	**Medium**	Set once
Change a password when compromise is suspected, not on a fixed timer	Forced changes every 90 days lead to predictable passwords such as Summer2026!. Windows expires passwords after 42 days unless you change that setting. If an auditor or contract requires periodic changes, use the longest interval allowed.	**Medium**	On suspicion
Block common and breached passwords	Check new passwords against a list of known breached passwords. Many password managers and directory services can do this.	**Medium**	Set once
No shared accounts	Every person has their own account, so every action can be traced to one person.	**High**	At onboarding
Least privilege	Staff get only the folders and rights their work needs. Not everyone needs every client folder or admin rights.	**High**	At account creation; reviewed quarterly
Disable accounts within 24 hours of someone leaving	A former employee's working password is a risk, even without bad intent. Use an offboarding checklist.	**High**	Every departure
Review all user accounts every quarter	Accounts of former staff, contractors and old services pile up.	**High**	Quarterly
Use multi-factor authentication for remote access and email	A second factor stops access with a stolen password. Start with admin accounts.	**High**	Always

4. Remote access

Remote Desktop open to the internet is one of the biggest risks for a small office. Automated tools try passwords against every exposed server around the clock.

Action	Why it matters	Priority	Frequency
Never leave Remote Desktop open to the internet	Bots probe every reachable server all day. Strong passwords alone do not make an exposed port safe.	**High**	Always
Put remote access behind a VPN	Staff connect to the VPN first, then to the server's private address. The server's Remote Desktop port is never visible from the internet.	**High**	Always
Allow Remote Desktop only from the VPN	A firewall rule that accepts Remote Desktop only from the VPN's address range closes the port to everyone else.	**High**	Always

Action	Why it matters	Priority	Frequency
Give each person their own VPN access	No shared access codes, so one person's access can be removed without affecting the rest.	**High**	Per person
Remove VPN access the day someone leaves	A former employee with VPN access can reach the server from anywhere.	**High**	Every departure
Control remote-support tools	Remote-support tools give full control of the server. Install them only when needed, remove them afterwards, and check the firewall is still on after any installation.	**High**	Every installation
Record who connects remotely	Who connected, when and from where. You will need it after an incident.	**High**	Ongoing
Lock idle sessions after 5 minutes	An unattended session is an open door.	**Medium**	Set once

5. Monitoring and alerting

Monitoring does not prevent attacks. It makes sure you hear about them while you can still limit the damage.

Action	Why it matters	Priority	Frequency
Turn on Windows audit policies	Windows must be told to record sign-ins, failures, account changes, policy changes and service installations, or the log stays incomplete.	**High**	Once
Alert on bursts of failed sign-ins	Many failures from one address in minutes is a password-guessing attack in progress.	**High**	Always on
Alert on administrator sign-ins outside working hours	An admin sign-in at 2 am is rarely expected. A prompt alert lets the Security Officer check it.	**High**	Always on
Alert on new accounts and changes to admin groups	Attackers often create a backdoor account or add themselves to Administrators.	**High**	Always on
Alert when the security log is cleared	Clearing the log is a standard way to hide what happened.	**High**	Always on
Alert when the firewall is switched off	A switched-off firewall exposes every service on the server.	**High**	Always on
Review new services and scheduled tasks	Malware often installs itself as a service or a scheduled task.	**Medium**	Daily
Read alerts the same day, high-severity ones within 2 hours	An alert read three days later rarely helps.	**High**	Daily
Block addresses that keep failing to sign in	Blocking repeat offenders at the firewall cuts noise and stops the attempt.	**High**	Always on

Action	Why it matters	Priority	Frequency
Send a weekly summary to the partners	A short, non-technical summary keeps management informed.	**Medium**	Weekly

6. Email and communication

Phishing is one of the most common ways attackers get in. A firm that receives client financial documents by email is a valuable target.

Action	Why it matters	Priority	Frequency
Use business email on your own domain	Free personal mailboxes are not suitable for client work, and a domain lets you set up authentication.	**High**	Once
Publish SPF, DKIM and DMARC records	With DMARC set to quarantine or reject, receiving mail services can refuse email that falsely uses your domain. They do not stop lookalike domains. Your email or hosting provider can set them up.	**High**	Once; checked every year
Verify payment and bank-detail changes by phone	Business email compromise imitates clients and colleagues. A call to a known number stops it.	**High**	Always
Be careful with unexpected attachments and links	Malicious Office and PDF files are a common delivery method. When in doubt, call the sender.	**High**	Always
Train staff to spot phishing	Cover urgency, mismatched sender addresses, unexpected attachments, and what to do after a wrong click.	**High**	Every year, with reminders
Report suspicious emails to the Security Officer	Early reports let the Security Officer warn everyone else.	**High**	Ongoing
Share sensitive documents by secure link, not attachment	Email is not end-to-end encrypted. Use a restricted link from your document storage or a client portal.	**Medium**	Always
Turn on spam and phishing filtering	Business email services include it; check it is on.	**High**	Once; checked every year

7. Data protection and backup

Ransomware encrypts your data and demands payment. A tested copy kept away from the server is the most reliable way to get your data back. It does not stop stolen data being leaked.

Action	Why it matters	Priority	Frequency
Back up all client data automatically every day	Manual backups get skipped.	**High**	Daily

Action	Why it matters	Priority	Frequency
Keep at least one copy off the server and offline or immutable	A backup the server can write to can be encrypted along with it.	**High**	Every backup
Test a restore every quarter	A backup you have never restored is a backup you do not have.	**High**	Quarterly
Encrypt backups	A lost or stolen backup drive should be unreadable. Keep the key safe and away from the backup: without it, the backup is lost too.	**High**	Always
Keep backups as long as your retention duties require	See the retention periods in the regulatory section: ordinarily at least seven years for audit documentation, and the statutory periods for tax and company records.	**High**	As required
Keep a retention and deletion schedule	Keeping data longer than needed increases what a breach exposes.	**Medium**	Reviewed every year
Keep client data off personal laptops and USB drives	Personal devices lack the server's protections and are easily lost.	**High**	Always
Encrypt the server's disks with BitLocker	A stolen server's data stays unreadable without the key. Save the recovery key somewhere safe, away from the server, before turning it on.	**Medium**	Once

8. Physical security

Physical access to a server gets around most digital controls.

Action	Why it matters	Priority	Frequency
Keep the server in a locked room or cabinet	The simplest and most effective physical control.	**High**	Always
Restrict and list who has the key	Remove access when people leave or change roles.	**High**	Reviewed quarterly
Lock screens automatically after 5 minutes	An unattended, signed-in screen is a risk.	**High**	Set once
Keep client files out of view in public areas	Visitors and couriers can read an unattended screen or desk.	**Medium**	Always
Clear desks and shred client papers	Printed documents leak too. Use a cross-cut shredder.	**Medium**	Always
Restrict USB storage on the server	USB drives bring malware in and carry data out. Disable autorun at the least.	**Medium**	Once
Never plug in a USB drive of unknown origin	Dropped or unsolicited drives are a known trick.	**High**	Training

9. Staff awareness and training

People are both the largest risk and the most effective control.

Action	Why it matters	Priority	Frequency
Cover this policy in every new joiner's induction	Passwords, phishing, physical security and what to do in an incident, before they get access to client data.	**High**	Every new joiner
Run security awareness training for everyone	Tactics change.	**High**	Every year
Run a phishing simulation	A harmless test email shows who needs more training.	**Medium**	Every year
Make reporting easy and blame-free	Incidents nobody reports are the ones that grow.	**High**	Always
Talk about security in team meetings	The Security Officer owns the policy; everyone carries it out.	**Medium**	Ongoing

10. Incident response

An incident is not a failure. A slow or improvised response is.

Action	Why it matters	Priority	Frequency
Define what counts as an incident	Ransomware, unauthorised access, a click on a phishing link, a lost laptop with client data, an attack alert nobody looked at.	**High**	In this policy
Write down who does what	Who is called first, who informs clients, who calls IT support, who reports to CERT-In. Keep the list where you can reach it if the server is down.	**High**	Once; reviewed every year
Report to CERT-In within 6 hours when required	The 6-hour clock runs from when you notice the incident or are told about it. Report as soon as you have the basic facts. Prepare the contact details and a short report template in advance.	**High**	Every reportable incident
Contain first, investigate second	Disconnect the affected machine from the network and keep its logs. Switch it off only if you cannot disconnect it: shutting down destroys evidence.	**High**	Training
Know when you must tell clients or the regulator	Today, CERT-In must be told of reportable incidents within six hours, and your engagement letters may require telling clients. From May 2027, the DPDP Act requires telling the Data Protection Board and every affected person of any personal data breach. Take legal advice on what to tell clients now.	**High**	Training
Record every incident in the Security Register	What happened, when it was found, what was done, and the outcome.	**High**	Every incident

Action	Why it matters	Priority	Frequency
Review each significant incident within 2 weeks	What worked, what did not, and what changes.	**High**	After each incident
Plan another way into the server	If Remote Desktop is unavailable you need the physical console or a second path.	**Medium**	Planned in advance

11. Vendors and software

Third-party software and suppliers are an often overlooked risk.

Action	Why it matters	Priority	Frequency
Keep a list of software installed on the server	Know what runs on it. Investigate anything new you did not install.	**Medium**	Reviewed quarterly
Install software only from the publisher	Pirated software and unofficial downloads often carry malware.	**High**	Always
Remove software nobody uses	Every installed program is something to patch or attack.	**Medium**	Quarterly
Give suppliers their own accounts and remove them afterwards	IT providers, software vendors and consultants should never share your credentials.	**High**	Per supplier; reviewed every year
Keep accounting and tax software up to date	Vendors fix security problems, and attackers target popular applications.	**High**	Each release
Use licensed software	Unlicensed copies may not get security updates.	**Medium**	Every year

12. Review and audit schedule

Activity	Frequency	Responsible
Read security alerts	Daily, same day	Security Officer
Review blocked addresses and unblock any legitimate ones	Weekly	Security Officer
Check all firewall profiles are on	Monthly	Security Officer
Review user and administrator accounts	Quarterly	Security Officer
Test a backup restore	Quarterly	Security Officer and IT support
Internal security review against this policy	Quarterly	Security Officer
Review physical access	Quarterly	Security Officer
Staff security training	Every year	Security Officer

Activity	Frequency	Responsible
Independent security audit	Every year	External consultant
Review and update this policy	Every year	Security Officer and partners
Review the retention schedule	Every year	Security Officer and compliance
Review suppliers and installed software	Every year	Security Officer
Check SPF, DKIM and DMARC records	Every year	IT provider
Review the incident log for patterns	Every year	Security Officer and partners

13. Where Prixl Warden helps, and where it does not

Prixl Warden is a monitoring and hardening agent for Windows servers, with Prixl Guard for private remote access. This is what it does today for the controls in this policy.

Policy area	What Prixl Warden does	What you still need
2. Server security	Checks the server's security settings and scores them out of 100. One-click fixes for: firewall on all profiles, SMBv1, Network Level Authentication, the Guest account, the Remote Desktop port, and PowerShell script block logging. Flags Defender status and Windows Update age, with guidance.	Installing updates; antivirus; disabling unused services.
3. Passwords	One-click fixes for minimum password length (enter 15, or 14 where Windows allows no more), password history and account lockout.	MFA; breached-password checks; account reviews.
4. Remote access	Prixl Guard: an encrypted private connection to the server, with a single-use invite code per person that the admin can revoke. "Lock RDP to Secure Access only" allows Remote Desktop only from the office network, Guard connections and addresses you trust.	MFA for the connection (Guard does not provide it yet); control of remote-support tools.
5. Monitoring	Turns on the audit policies it needs. Immediate email for: a sign-in that succeeds after repeated failures, admin sign-ins outside working hours, new user accounts, changes to Administrators and Remote Desktop Users, the security log being cleared, and the firewall being switched off. Password-guessing attacks, other account changes, new services and new scheduled tasks are reported in a daily digest. Automatic blocking of repeat offenders, with a threshold you set. A weekly summary email.	Reading and acting on alerts.
1, 10. Governance and incidents	The dashboard's Activity tab records changes made through the dashboard. Alerts and digests are a written record of security events.	The Security Register, the response plan and CERT-In reporting.
CERT-In 180-day logs	Not provided today. Warden keeps the security events it watches, not complete Windows log files.	A daily export of full Windows logs to storage in India.
6, 7, 8, 9. Email, backup, physical, training	Not covered.	Your email provider, backup software, physical controls and training.

PRIXL

About Prixl. Prixl Technologies builds Prixl Warden, which watches and hardens the Windows servers of small professional firms and alerts the partners when something needs attention, and Prixl Guard for private remote access. Learn more at prixl.io. The latest version of this policy is at prixl.io/security-policy. Questions: support@prixl.io.

You may copy, adapt and share this document, including with other firms, under the Creative Commons Attribution 4.0 International licence (CC BY 4.0, creativecommons.org/licenses/by/4.0): credit Prixl Technologies, link to the licence and say if you changed it. The Prixl name and logo are not licensed. This summary of laws is for general awareness only and is not legal advice.