

Password and Authentication Policy Template

For Jamaican organizations. Prepared by Syxel Technologies Limited.

How to use this template

This template gives you a complete starting point for a password and authentication policy. It follows NIST Special Publication 800-63B-4, the United States National Institute of Standards and Technology guidance on authentication published in 2025, which is widely used as a reference by organizations around the world. Delete this page before you adopt the policy.

- Replace everything in **[square brackets]** with your own details, and delete examples that do not apply.
- Decide who owns the policy. In a small organization this is often the operations manager working with your IT staff or IT provider.
- List your systems in the MFA Coverage Register (Appendix A) and record whether multi-factor authentication is turned on for each one. Gaps on email, remote access, admin accounts and finance systems should be fixed first.
- List every shared and service account in Appendix B, with a named owner for each.
- Check what your systems can actually enforce, such as minimum length, banned password lists and lockout settings, and adjust the numbers in sections 5 and 11 if a system cannot meet them. Record any gap as an exception (section 15).
- Choose and roll out a password manager before you ask staff to use longer, unique passwords. It is much easier to follow the policy with one.
- Train staff on the policy, give them the quick guide in Appendix C, and collect signed acknowledgements (Appendix D).

Some older audit checklists, insurers or client contracts still ask for regular forced password changes or complexity rules. If one applies to you, record it as an exception in section 15 rather than applying it to every account.

This template is general guidance, not legal advice. It was prepared by Syxel Security, the cybersecurity team at Syxel Technologies Limited. For help adapting it, setting up multi-factor authentication or training your staff, contact sales@syxeltech.com.

[Organization] Password and Authentication Policy

Policy owner	[Role, e.g. Operations Manager or IT Manager]
Approved by	[Name, role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, 12 months after the effective date]

1. Purpose

Most break-ins to business systems start with a stolen, guessed or reused password. This policy sets out how people working for [Organization] create, protect and use passwords and other sign-in methods, so that our email, money, customer information and systems are harder to break into.

The rules follow current international guidance (NIST SP 800-63B-4). That guidance favours long passwords, checks against known breached passwords and multi-factor authentication. It discourages forced periodic changes and complicated character rules, because they lead people to choose predictable passwords and write them down.

2. Scope

This policy applies to:

- all employees, contractors, consultants, interns and volunteers who have an account on any [Organization] system;
- all accounts used for [Organization] work, including email, computers and phones, file storage, finance and banking, payroll and HR, customer systems, social media pages, websites, domain names and cloud services;
- devices with a login or admin page, including routers, firewalls, Wi-Fi access points, CCTV recorders and cameras, access control systems, printers and UPS units;
- IT staff and IT providers who set up, manage or support these systems.

3. Definitions

Term	Meaning
Password	A secret made of characters that you type to prove who you are. In this policy it includes passphrases and PINs used to sign in to systems.
Passphrase	A password made of several words, such as four random words with spaces or hyphens between them. Passphrases are long, which makes them strong, and easier to remember than short random strings.
Multi-factor authentication (MFA)	Signing in with two or more different types of proof: something you know (a password), something you have (a phone app, security key or passkey on a device) or something you are (a fingerprint or face).
Phishing-resistant MFA	MFA that cannot be passed to a fake website, such as passkeys and hardware security keys. Codes sent by text message and approve-or-deny prompts can be tricked out of people; phishing-resistant methods cannot.
Password manager	An approved app that creates, stores and fills in passwords securely, protected by one strong main password and MFA.
Shared account	An account that more than one person signs in to, such as a front-desk computer login or a social media page login.
Service account	An account used by a system or application rather than a person, for example to run backups or connect two systems.
Privileged account	Any account with admin rights: it can change settings, create users, reset passwords, install software or reach all data on a system.
Default password	The password a device or system ships with from the manufacturer. These are often published online.

4. Roles and responsibilities

Role	Responsibilities
Policy owner: [role]	Keeps this policy and the registers in Appendices A and B up to date, approves exceptions, arranges training and reviews the policy.
IT staff or IT provider: [name or company]	Configures systems to enforce this policy where they can, manages privileged and service accounts, resets passwords and MFA securely, and changes default passwords on all devices.
Managers	Make sure their teams follow this policy, approve access for new staff, and tell [role] straight away when someone changes role or leaves.

Role	Responsibilities
HR or [role]	Tells IT in advance about new starters and leavers so that accounts are created and removed on time.
Everyone covered by this policy	Follows this policy, keeps their passwords and MFA devices to themselves, uses the password manager, and reports suspicious messages and possible compromises straight away.

5. Password length and passphrases

Length is what makes a password strong. Use these minimums wherever a system allows it:

Type of account	Minimum length
Any account that relies on a password alone (no MFA)	15 characters
Accounts protected by MFA	[12] characters, and never fewer than 8
Privileged and admin accounts	15 characters, always with MFA
Password manager main password	15 characters, always with MFA
Service accounts and device admin logins	[25] characters, randomly generated by the password manager

- A passphrase of four or more random words is the easiest way to meet these lengths. Do not use a well-known phrase, quote, song lyric or the example in our training material.
- You may use any characters, including spaces. You do not have to include capitals, numbers or symbols, and [Organization] systems will not demand them where we can turn that rule off.
- Systems should accept passwords of at least 64 characters, allow pasting and allow password managers to fill them in. IT will configure this where the system allows it.
- Use a different password for every account. Never reuse a work password anywhere else, and never use a personal password for work.
- Passwords do not expire on a schedule. You only need to change a password when there is a reason to (section 11).

6. Banned and breached passwords

Criminals try common passwords and passwords leaked from other websites first. You must not use a password that:

- appears in a list of breached or commonly used passwords, such as "Password1", "Welcome123" or "Qwerty2025";
- includes [Organization]'s name, our products, our street or town, or a word that guessers would try for us, such as the parish, a local sports team or "Jamaica" with a year;
- includes your name, username, date of birth, phone number, TRN, children's or pets' names;
- is a keyboard pattern or repeated characters, such as "1234567890" or "aaaaaa";
- is an old password with a small change, such as a new number or season at the end.

Where our systems support it, IT will turn on checks that reject breached and banned passwords when they are set, and will add [Organization]-specific words to the banned list. If a system rejects your password, it will tell you why; choose a different one rather than adding a number.

The password manager may warn you that a saved password has appeared in a breach. If it does, change that password straight away and tell [role] if it is a work account.

7. Multi-factor authentication

MFA stops most attacks that use stolen passwords. It must be turned on for the systems below, for every user, including managers and directors. Appendix A records where it is in place.

System	MFA required	Notes
Email, including webmail and phone email apps	Yes, everyone	Email is used to reset other passwords and to trick customers and suppliers, so it is the most important account to protect.
Remote access: VPN, remote desktop and remote support tools	Yes, everyone	Including IT providers and vendors who connect to our systems.
Admin and privileged accounts	Yes, phishing-resistant where the system supports it	See section 10.
Finance systems: online banking, accounting, payroll and payment platforms	Yes, everyone	Use the bank's own token or app where one is offered.
Password manager	Yes, everyone	It holds the keys to everything else.
Cloud file storage, HR and customer systems	Yes, everyone	
Website hosting, domain name and DNS accounts	Yes	Losing these can take down our website and email.

System	MFA required	Notes
Company social media pages and messaging accounts	Yes	Turn on two-step verification in each app.
CCTV and access control apps with remote viewing	Yes, where supported	
[Other systems]	[Yes or no]	

Use the strongest method each system offers, in this order:

- Passkeys or hardware security keys. These are phishing-resistant and are required for admin accounts where the system supports them.
- An authenticator app on your work or registered phone, preferably with number matching, where you type the number shown on screen.
- A code sent by text message or voice call, only where nothing better is available. NIST restricts this method because phone numbers can be stolen through SIM swaps. Tell [role] if a system only offers this.
- Never approve an MFA prompt or read out a code that you did not request. Deny it and report it straight away: it means someone has your password.
- Never give an MFA code to anyone who calls, texts or emails you, even if they say they are from IT, your bank or a supplier.
- Tell [role] straight away if you lose the phone or security key you use for MFA, or change your phone number.

8. Password managers

- [Organization] provides [name of password manager] for work passwords. Use it to create and store every work password except the main password for the password manager itself and your computer login.
- Let the password manager generate random passwords for accounts you do not type into by hand.
- Protect the password manager with a passphrase of at least 15 characters that you use nowhere else, and with MFA.
- Share passwords with colleagues only through the password manager's sharing feature, never by email, text message, WhatsApp, paper or spreadsheet.
- Do not save work passwords in a personal password manager or in a web browser on a personal device. [Saving passwords in the browser on work devices is / is not allowed.]
- If you leave [Organization], the work vault stays with [Organization]. Do not export it.

9. Shared and service accounts

Every person should have their own account, so we know who did what and can remove access when someone leaves. Shared accounts are allowed only where a system cannot support individual accounts, and only with [role]'s approval.

- Every shared and service account is listed in Appendix B with a named owner.
- Shared account passwords are kept in a shared folder in the password manager, available only to the people who need them.
- Shared accounts use MFA where the system allows it, for example by linking the account to a shared authenticator managed by the owner.
- When someone who knew a shared password leaves or changes role, the owner changes the password within [1 working day].
- Service accounts use long random passwords or keys, have only the access they need, and cannot be used to sign in interactively or read email unless that is required.
- Passwords and keys for service accounts are never written into scripts, configuration files or source code in plain text. IT stores them in the password manager or a secrets vault.
- [Role] reviews Appendix B every [6] months and removes accounts that are no longer needed.

10. Admin and privileged accounts

- People who need admin rights get a separate admin account, used only for admin tasks. Their everyday account, used for email and browsing, has no admin rights.
- Admin accounts use a password of at least 15 characters and MFA, phishing-resistant (passkey or security key) wherever the system supports it.
- Do not read email, browse the web or open attachments while signed in as an admin.
- Admin rights are given only with [role]'s approval and only for the systems the person needs. [Role] reviews the list of admin accounts every [3] months.
- Staff do not have admin rights on their own computers unless [role] approves it.
- IT providers and vendors use named accounts, not a shared admin login, and their access is removed when the work ends.
- Keep [one or two] emergency ("break glass") admin accounts for when normal sign-in fails. Store their details securely [in a sealed envelope in the safe / in a separate password manager vault], use them only in an emergency, and change the password after each use.

11. Resets, changes and lockouts

You must change a password, and tell [role], straight away if:

- you think someone else knows it or has used it;

- you typed it into a website or form that may have been fake;
- the password manager, a breach notice or IT tells you it has been exposed;
- you used it for any other account;
- it is a shared password and someone who knew it has left or changed role.

Otherwise, passwords do not need to be changed on a schedule.

Rules for IT staff and anyone who resets passwords or MFA:

- Confirm the person's identity before any password or MFA reset. Do not rely on a caller's word, a caller ID, a voice or an email alone. Use [an approved method, e.g. calling back on the number in the staff directory, confirming in person, or confirmation from their manager].
- Treat requests to reset MFA or register a new phone with extra care. They are a common way for attackers to take over accounts.
- Temporary passwords are random, given only to the account holder, work once, and must be changed at first sign-in.
- Self-service password reset, where offered, must itself require MFA. Do not use security questions or password hints.
- Systems lock or slow down sign-in after [10] failed attempts in a row [for 15 minutes]. Repeated lockouts are reported to [role] as a possible attack.

12. Default passwords on devices

Routers, Wi-Fi access points, firewalls, CCTV recorders (DVRs and NVRs), IP cameras, access control panels, printers, UPS network cards and similar devices often ship with a default password that is printed in the manual and published online. Criminals scan the internet for them. Before any device is put into use, the person installing it, whether our staff or an installer, must complete these steps:

- ☐ Change the default admin password to a unique, randomly generated password of at least [20] characters.
- ☐ Rename or disable the default admin username where the device allows it.
- ☐ Change the default Wi-Fi network name and password, and turn off WPS.
- ☐ Turn off remote access, cloud viewing and peer-to-peer (P2P) features that are not needed. Where remote viewing of CCTV is needed, protect the app account with a strong password and MFA.
- ☐ Install the latest firmware update, and turn on automatic updates where available.
- ☐ Store the admin login in the password manager, not on a sticker on the device or in the installer's notebook.
- ☐ Record the device, its location and who holds the admin login in [the asset register / Appendix B].

IT will check existing devices against this list by [date] and every [12] months after that. Installers and contractors must hand over all admin logins when their work is complete, and we change them afterwards.

13. Storing and sharing passwords

- Keep passwords in the password manager. Do not write them on sticky notes, in notebooks, on whiteboards, in spreadsheets, in documents or in phone notes.
- Never send a password by email, text message, WhatsApp or other messaging app. If you must give someone a password, use the password manager's sharing feature, or give it in person or by phone and ask them to change it.
- Never tell anyone your own password, including your manager, colleagues or IT. IT will never ask for it.
- Do not let anyone watch you type a password, and do not use "remember me" on shared or public computers.
- Systems we build or buy must store passwords only as salted hashes using a recognized password hashing method, never in plain text or in a form that can be turned back into the password. Ask suppliers to confirm this before we buy.

14. Phishing and reporting

Phishing emails, texts, WhatsApp messages and calls try to trick you into typing your password or MFA code into a fake page or reading it out. No password rule protects you if you give it away.

- Before typing a password, check that the website address is correct. When in doubt, go to the site yourself, using a bookmark or by typing the address, rather than clicking a link.
- Be suspicious of messages that create urgency: an account about to close, a missed delivery, an unpaid invoice, a new voicemail or a shared document you were not expecting.
- Report suspicious messages to [role, email or report button] and then delete them. Do not forward them to colleagues.
- If you entered your password or MFA code on a suspicious page, or approved a prompt you did not expect, change your password straight away and report it to [role, email and phone number]. Reporting quickly limits the damage, and you will not be penalized for an honest mistake reported promptly.

If an account that holds personal data may have been compromised, [role] will decide whether it is a personal data breach. The Data Protection Act, 2020 requires certain breaches to be reported to the Information Commissioner within 72 hours of becoming aware of them, so do not wait to report.

15. Exceptions and enforcement

- If a system cannot meet this policy, for example because it does not support MFA or long passwords, [role] records the exception in Appendix A or B, with the reason, the extra safeguards in place, an expiry date and who approved it.
- Exceptions are reviewed at least every [12] months, and when the system is upgraded or replaced.
- IT may check that this policy is followed, for example by reviewing MFA coverage, admin accounts and password settings, in line with our [IT acceptable use policy].
- Breaking this policy may lead to loss of access and to disciplinary action under our [disciplinary policy]. Deliberately sharing passwords, getting around MFA or using someone else's account are serious breaches.

[Role] reviews this policy every [12] months, or sooner if NIST guidance, our systems or our risks change. Related policies: [IT Acceptable Use Policy; AI Acceptable Use Policy; Information Security Policy; Data Protection and Privacy Policy; Incident Response Plan; Disciplinary Policy].

Appendix A: MFA Coverage Register

[Role] keeps this register up to date and reviews it every [6] months. Fix gaps on email, remote access, admin accounts and finance systems first.

System	Who uses it	MFA on for all users? (yes, no, partly)	MFA method	Exceptions, safeguards and expiry	Checked by and date
[e.g. Email]	[e.g. All staff]		[e.g. Authenticator app]		
[e.g. Remote access / VPN]					
[e.g. Online banking]					
[e.g. Accounting and payroll]					
[e.g. Admin accounts]					
[e.g. Password manager]					

Appendix B: Shared and Service Account Register

List every shared login, service account, emergency admin account and device admin login. Store the passwords in the password manager, never in this register.

Account or device	Type (shared, service, emergency, device)	Purpose	Owner	Who has access	MFA? (yes or no)	Password last changed	Next review
[e.g. Front desk PC login]	[Shared]		[Name]				
[e.g. Backup service account]	[Service]						
[e.g. CCTV recorder admin]	[Device]						

Appendix C: Quick Guide for Staff

The five things that matter most: long passphrases, a different password for every account, the password manager, MFA on everything important, and reporting anything suspicious straight away.

Do	Don't
Use a passphrase of four or more random words	Use names, birthdays, "Jamaica" plus a year or our company name
Use a different password for every account	Reuse a work password anywhere else
Keep passwords in [password manager]	Write passwords down or keep them in a spreadsheet
Turn on MFA and use the authenticator app	Approve a sign-in prompt you did not start
Change a password straight away if it may be exposed	Change passwords just by adding a number
Check the website address before signing in	Click sign-in links in unexpected messages
Share logins only through the password manager	Send passwords by email, text or WhatsApp
Report suspicious messages to [role]	Give your password or MFA code to anyone, even IT

Need help? Contact [role, email and phone number].

Appendix D: Staff Acknowledgement

I have read and understood the [Organization] Password and Authentication Policy, version [1.0], and I agree to follow it. I understand that breaking it may lead to disciplinary action.

- ☐ I have set up multi-factor authentication on my work accounts.
- ☐ I have been given access to the password manager and know how to use it.
- ☐ I know how to report a suspicious message or a possible compromise.

Name	
Role and department	
Signature	
Date	