

The Modern Perimeter

SECURING CLOUD IDENTITY AND SERVICES



The footprint of modern elections is broader than ever. The infrastructure that enables elections no longer only sits on premises. Much of the work of preparing for and running elections now depends on cloud services: email, file sharing, voter registration access, online voter services, election night reporting tools, candidate portals, vendor support portals, domain and website administration, and official social media accounts. In many cases, these cloud services can offer stronger security than offices could build on their own, but securing cloud environments requires additional attention to identity, session management, and monitoring. This is not a comprehensive guide on cloud security; rather, it focuses on essential practices for securing the logins and the services behind them.

The Risk: Why Identity Matters

Sometimes, attackers just sign in. A stolen password, an old account, a vendor's session token, or an administrator account with more access than it needs can give an attacker a path into election-related cloud services and systems. To systems, these logins may look normal. The username is right, the password is right, and the session is valid. Without proper configuration, the services alone cannot distinguish between the correct person with their credentials and the wrong person using those same credentials.

That is why cloud identity has become part of election infrastructure. Protecting accounts is part of protecting voter data, official communications, election reporting, public confidence, and continuity of operations.

A cloud system is a network of remote, virtualized computing resources including processing power, storage, databases, networking, and software, that is delivered over the internet on an as-needed basis. Instead of buying, owning, and maintaining physical servers or local hardware, you rent access to these services from a cloud provider.

Resources:

NIST SP 800-145, [The NIST Definition of Cloud Computing](#)

Amazon Web Services, [What is Cloud Infrastructure?](#)



The Starting Point: Know the Cloud Footprint

Cloud accounts multiply quietly. Every office and vendor should keep a current inventory of cloud systems used for election work. The inventory does not need to be fancy; a simple spreadsheet is enough, if a solution does not already exist. For each service and system, the office should know who has access, who has administrator rights, who approves new accounts, how accounts are removed, and who can review logs.

At minimum, the inventory should include:

- Email and office productivity systems
- File-sharing and document storage tools
- Voter registration access portals
- Online voter services
- Election night reporting tools
- Electronic pollbook management and support systems
- Vendor support portals
- Website administration tools
- Domain registrar and DNS accounts
- Official social media accounts
- Remote access tools
- Service accounts, API keys, and other non-human access



This step is critical to understanding risk: who can sign in, what can they reach, and why do they need access? Understanding these factors helps identify which accounts reach the most consequential systems and data so those accounts can be prioritized for protection and monitoring.

Accounts that would cause the most harm if stolen usually include:

- Administrator accounts
- Election night reporting accounts
- State voter registration system accounts
- Email administrator accounts
- Vendor support and engineering accounts
- Domain registrar and DNS administrator accounts
- Accounts that manage official websites or social media
- Accounts that can create users or reset passwords
- Accounts that can export sensitive election data

Protect the Highest-Risk Accounts First

Accounts that can publish unofficial results, reset passwords, change voter registration data, approve new users, administer email, or control a public-facing election domain deserve stronger protection than a read-only account used for routine work.

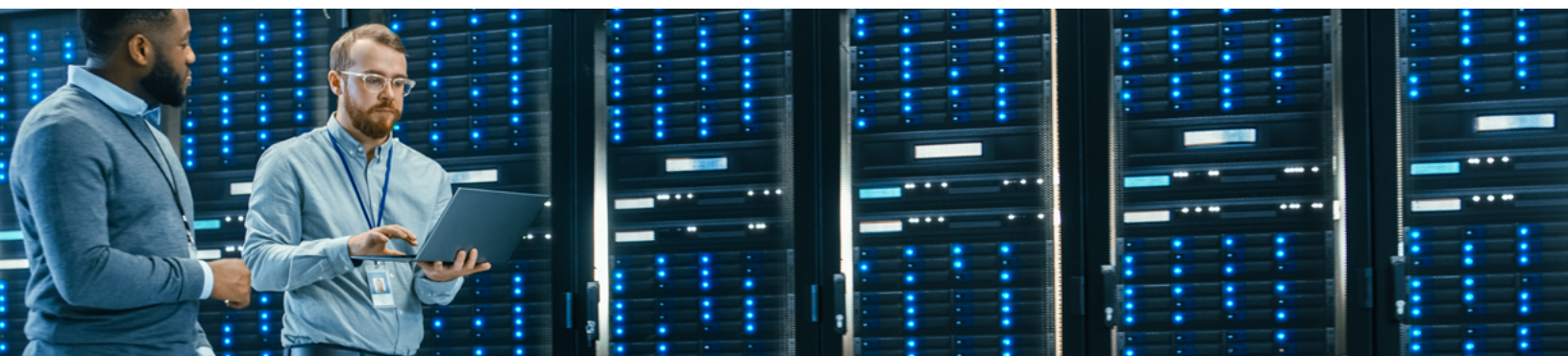
Every account used for election work should have multi-factor authentication, or MFA. MFA means a second check beyond a password. That second check might be an app prompt, a code, a passkey, or a hardware security key. **CISA** estimates that turning on MFA makes an account about 99 percent less likely to be compromised, which makes it one of the most valuable steps an office can take.

But MFA is not all the same. Text-message codes are better than a password alone, but they are easier to defeat than stronger methods, because a texted code can be intercepted. Push notifications can be abused when attackers flood a user with approval requests until one is tapped by mistake, a tactic sometimes called MFA fatigue. Phishing-resistant MFA, such as a passkey or hardware security key or number matching (where you have to type the number from your computer onto your phone), is stronger because it helps confirm that the user is signing in to the real site, not a look-alike phishing page.

The strongest controls should secure the accounts that matter most.

Key practices:

- Require phishing-resistant MFA for every account used for election work.
- Use phishing-resistant MFA for administrator, reporting, vendor support, and other high-risk accounts. If the vendor does not support it, ask them to.
- Do not exempt senior staff, executives, or long-tenured employees.
- Give each account the least access its work requires. Extra rights are rarely noticed until they are used.
- Give administrators a separate account for administrator work.
- Do not let staff read email or browse the web using an account with elevated privileges.
- Turn off older login methods that bypass MFA.
- Block passwords that have appeared in known breaches, where the platform supports it.
- Review account recovery options, backup codes, and secondary email addresses.
- Remove access the same day someone leaves, including temporary and seasonal workers.



Control Sessions, Not Just Passwords

A login is only the beginning. After someone signs in, most cloud services create a session. A session is what lets the user keep working without typing a password on every click. The service remembers that the user has already authenticated.

That session can be stolen. Malware on a computer can steal it. A phishing site can capture it. A poorly managed device can expose it. Once an attacker has a valid session, they may not need the password again. They may not need to pass MFA again.

This is why a password reset is not always enough. If an attacker still has an active session, they may still be inside. **The same problem applies if an attacker has connected an outside application** to the account. That connection can keep working after the password changes, so it has to be found and removed on its own.

Sensitive election systems should have stronger session rules than routine systems. A user should not stay signed in indefinitely to an account that can publish results, administer users, change voter records, or access sensitive files.

Key practices:

- Use shorter session lifetimes for sensitive systems.
- Require a fresh login before high-impact actions.
- Revoke all active sessions when an account may be compromised.
- Do not rely only on a password reset.
- Sign out of sensitive systems when work is complete, especially on shared or temporary devices.
- Limit persistent sessions on administrator accounts.
- Watch for sessions appearing from unfamiliar devices, locations, or networks.
- Vendors should also design their systems so sessions can be revoked quickly, sensitive actions require fresh authentication, and customer support access can be traced to a named person.

Configure Cloud Services Deliberately

Cloud services arrive configured for convenience. Sharing is easy, features are on, and setup is fast. Those defaults are chosen to help a new customer get started but, left unchanged, they could put data at risk.

Configuration is one of the most common ways cloud systems end up exposed. Examples include file-sharing folders with permissions that are too permissive (e.g. accessible via public link), storage locations made public during setup, or lingering test accounts.

Configuration is a decision, even when nobody consciously makes it. The goal is to make those decisions on purpose, write them down, and check them again after every major change.

Key practices:

- Review sharing settings on email and file storage. Know whether staff can share outside the organization, and whether links work for anyone who holds them.
- Find out what is publicly reachable. Storage locations, administrative consoles, and test sites should not be open to the internet unless someone decided they should be.
- Turn off what is not used, including old sign-in methods and integrations nobody remembers approving.
- Remove test accounts, sample data, and setup credentials once a system is live.
- Use the security checkup tools built into the major platforms. They compare your settings against a recommended baseline, and they are usually free.
- Enable phishing-resistant multi-factor authentication for all accounts.
- Protect the domain itself. Lock the registrar account, turn on auto-renew so the domain cannot lapse, limit who can change DNS records, and list more than one administrative contact for redundancy. Treat these credentials as high-risk.
- Turn on email authentication (SPF, DKIM, and DMARC). These settings let other mail systems verify that a message claiming to come from your domain actually did. This makes it harder for anyone to send a fake email in your name.
- Recheck settings after platform updates. New features sometimes arrive turned on.
- Vendors: ship secure defaults. Customers should have to opt out of security, not into it.
- Document the reasons for settings that depart from the baseline, so the next administrator does not quietly undo a decision that mattered.

Manage Vendor Access

Many election systems are hosted, maintained, or supported by vendors, meaning vendor employees may be able to reach election data, support portals, reporting systems, or administrative tools. If that access is necessary, it should be monitored and managed.

Questions to ask vendors:

- Which vendor employees can access our systems or data?
- Are vendor accounts assigned to named individuals?
- Are any shared accounts used?
- Is phishing-resistant MFA required for all vendor employees?
- Is phishing-resistant MFA required for vendor administrators or support staff?
- Can vendor access be limited to approved support windows?
- Are support sessions logged?



- Can we review logs after an incident?
- How quickly will the vendor notify us if one of its accounts is compromised?
- How is one customer's data separated from another's?
- How are former vendor employees removed from access?
- Contracts should require named accounts, phishing-resistant MFA, timely removal of access, breach notification, logging, least-privilege access, and the ability to review vendor access related to election systems or data.

When comparing vendors, ask whether they hold an independent security review, such as SOC 2 Type 2, or government authorization, such as **FedRAMP** or **GovRAMP** (formerly StateRAMP). These are useful signals that a vendor takes security seriously, but they are not guarantees. Confirm that the review covers the specific product your office will use, not just the company as a whole.

For high-risk systems, standing access should be avoided where practical. Vendor access should be approved when needed, logged while in use, and removed when the work is complete.

Watch for Account Misuse

Cloud systems often record the evidence needed to spot account takeover. The problem is that many offices do not know which logs are turned on, how long they are kept, or who is supposed to review them.

Useful alerts include:

- A new administrator account is created.
- MFA methods are added, removed, or changed.
- A password is reset unexpectedly.
- A dormant account becomes active.
- A user signs in from an unfamiliar device or location.
- A high-risk account signs in outside normal work patterns.
- A new email forwarding rule is created.
- A user grants an outside application access to email or files.
- A large number of files are downloaded or shared externally.
- A vendor support account is used without an open support request.

Logs are also important after an incident. They help answer what happened, which systems were touched, what data may have been accessed, and whether public communication is needed.

Key practices:

- Turn on sign-in, audit, and administrator activity logs where available.
- Keep logs long enough to investigate incidents discovered after an election.
- Decide who receives high-priority alerts.
- Review access before and after each election.
- Remove temporary accounts after each election.
- Review third-party application permissions.
- Require vendors to retain and provide logs for their access to election systems.
- Small offices should not be expected to do all of this alone. State partners, county IT, managed service providers, and vendors may all have roles. What matters is that the responsibility is assigned before there is a problem.

Plan for Account Takeover

In an increasingly cloud-dependent world, assume that, at some point, an account will be compromised and plan how to respond. Every organization involved in election work should have an account-takeover checklist.

A password reset is only one step. If the attacker added an MFA method, created a forwarding rule, approved a third-party app, or kept an active session, access may continue after the password changes.

Account-takeover checklist:

- | | |
|---|--|
| ☐ Revoke all active sessions. | ☐ Identify what data or systems were accessed. |
| ☐ Reset the password. | ☐ Preserve logs. |
| ☐ Remove unauthorized MFA methods. | ☐ Notify affected partners and vendors. |
| ☐ Check account recovery settings. | ☐ Decide whether public communication is needed. |
| ☐ Remove suspicious forwarding rules. | ☐ Document what happened and what changed after the incident. |
| ☐ Remove suspicious third-party app permissions. | |
| ☐ Review recent sign-ins. | |
| ☐ Review administrator activity. | |

Offices should also maintain a break-glass administrator account. This is an emergency account used only when normal administrator access is unavailable. Its credentials should be stored securely, protected with strong authentication where possible, and reviewed every time it is used.

Where to Get Help

Offices do not have to secure the cloud alone, and some of the strongest protections are free or low cost. The programs below are available to election offices at the time this guide was written. This landscape is changing quickly, though, so confirm that a program is still offered before relying on it.

- **.gov domains**: A .gov web address is limited to verified organizations and signals to the public that a site is official.
- **Cloudflare Athenian Project**: Protection available for state and local election and voter registration websites.
- **Microsoft AccountGuard**: It provides alerts and support against sophisticated threats for offices that use Microsoft 365.
- **Google Advanced Protection Program**: A security program for high-risk users, including election workers.
- **First Things First Cybersecurity Fast Wins for Election Offices**: A guide from the Election Security Exchange highlighting quick wins to boost cybersecurity in the office.
- **CISA's Implementing Phishing-Resistant MFA**: A factsheet introducing MFA and implementing options that are more resistant to phishing threats.
- **Trustworthy Email, NIST SP 800-177**: Technical guidance document with recommendations and guidelines for enhancing trust in email from the National Institute of Standards and Technology.

Technical Guidance

- The resources listed below are intended for technical audiences, such as system administrators, network managers, and information security specialists.
- NIST SP 800-63 (**Digital Identity Guidelines**): The NIST benchmark for identity proofing, authentication enablers, and federation management.
- NIST SP 800-210 (**General Access Control Guidance for Cloud Computing**): Focuses explicitly on access control models (RBAC, ABAC) across IaaS, PaaS, and SaaS.
- Cloud Security Alliance, **Security Guidance for Critical Areas of Focus in Cloud Computing**: Focuses heavily on Identity and Access Management and Infrastructure/Virtualization Security.