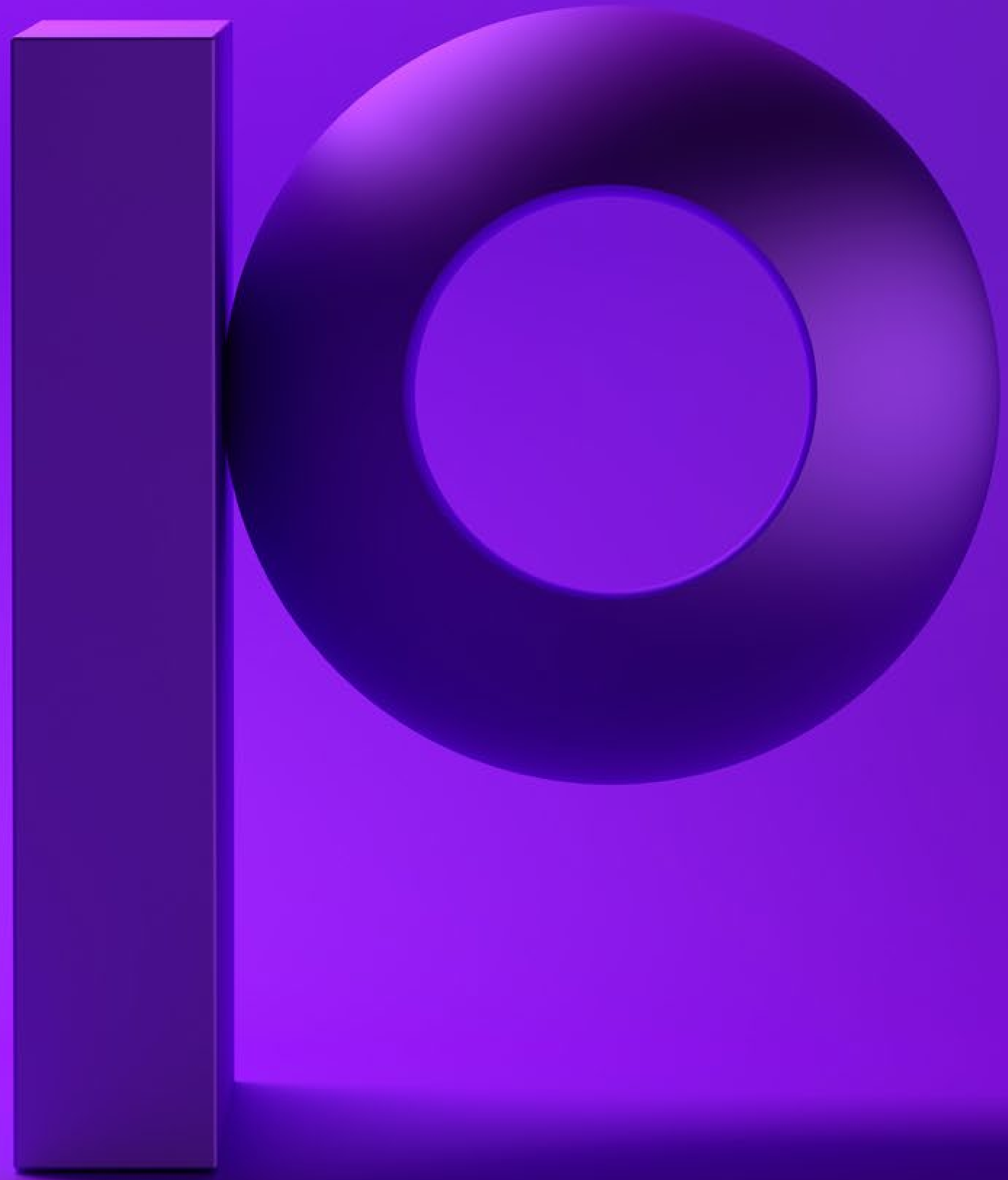
precisely

# Five IT Security Best Practices Derived from 23 NYCRR 500

New York's Tough Cybersecurity Law for Financial Services Companies May Soon Spread to Other States. What Every Company Can Learn About Strengthening IT Security from These New Regulations.



# Introduction

Given the frequency of high-profile data breaches, there's not likely to be any let-up in the pipeline of new and expanding compliance regulations that are forcing management and IT staff to strengthen their security posture. One of the newest laws affects a large number of companies that do business in the state of New York. Put forward by the New York State Department of Financial Services (NYDFS), regulation 23 NYCRR 500 outlines numerous provisions aimed at forcing financial-services companies to be significantly more diligent in their efforts to reduce data breaches and the subsequent exposure of sensitive customer information. Nearly all state-chartered banks, licensed lenders, private bankers, foreign banks, mortgage companies, and insurance companies operating in New York are affected. In addition, third-party service providers contracted by these regulated companies may also be required to meet compliance requirements, especially if these service providers store, process, or otherwise have access to the sensitive data of regulated companies.

Even those companies not required to comply with 23 NYCRR 500 should pay close attention as several other states are looking at following New York's lead. California, for example, has enacted expansive regulations under the California Consumer Privacy Act, which goes into effect in 2020 and impacts every industry operating in the state, not just financial services. The law is designed to force companies to protect sensitive consumer data in similar ways to Europe's General Data Protection Regulation (GDPR), and in Washington, D.C., there are

members of congress who would like to enact legislation at the national level that addresses data protection and privacy. Simply put, if your company hasn't yet been mandated to strengthen IT security by one or more compliance regulations, this will likely occur sometime in the near future.

The 23 NYCRR 500 regulation can serve as instructive guidelines for management and IT staff at companies in any industry who are ready to be proactive about security. To assist, this e-book highlights five general IT security best practices that can be derived from 23 NYCRR 500. These are:

1. Create and implement a detailed cybersecurity policy and plan.
2. Designate experts who take bottom-line responsibility for security and compliance.
3. Regularly assess risk, and test systems for vulnerabilities.
4. Implement technologies and processes that prevent unauthorized system access and the exposure of sensitive data.
5. Monitor systems for cybersecurity events, implement audit trails, and have an incident response plan.

Let's look more closely at these important security best practices as well as summaries of what's contained in the corresponding sections of 23 NYCRR 500.

# Best practice #1: Create and Implement a Detailed Cybersecurity Policy and Plan

At the heart of the regulation—and really of every sound IT security strategy—is the necessity for companies to develop and implement comprehensive cybersecurity policies and plans that not only aim at preventing a breach but also detail the steps to take in case a breach occurs. Without comprehensive, documented security plans and policies, as well as the careful education and training of staff, a company is more likely to take a "band-aid" approach to addressing security vulnerabilities, which inevitably creates gaps.

Some key areas that are typically included in IT security policies and plans:

- Physical security of data centers and IT equipment
- Network security
- Server-access controls
- Privileged-user account policies
- Configuration-change policies
- Logging of system configuration and data changes
- Mobile-device security policies
- Password policies
- Locations where different types of data are to be stored
- Procedures and reporting responsibilities in the event of a breach (incident-response plan)

Many IT managers design their cybersecurity plans and policies based on a formal, documented IT security risk assessment. In fact, a recent IT security survey conducted by Precisely found that 72% of respondents used the results of a security audit to define their organization's security program. In other words, when an effort is made to identify all of a company's IT security risks, appropriate policies and procedures that address those risks can be more effectively created, monitored, and enforced. More about security risk assessments later in this e-book.

**A summary of the specific regulations of 23 NYCRR 500 that correspond to this best practice:**

### 500.02 Cybersecurity Program

A sound cybersecurity program should be "designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems." The program should be based on your company's own risk assessment and must also include the activities of third-party IT service providers.

### 500.03 Cybersecurity Policy

Each covered company must create and enact a cybersecurity policy across the company that is approved by highest levels of management and that covers, among other things, data governance, user behavior, network security, and third-party IT service providers.

# Best practice #2: Designate Experts Who Take Bottom-line Responsibility for Security and Compliance

Implementing appropriate security technologies is important, but it is equally important for every company to have access to people with a high level of security and compliance expertise. These folks specialize in being able to efficiently and proactively find and close vulnerabilities within IT systems while regularly monitoring for any activity that might be suspicious. Not every company can afford to have in-house experts, which is why many use trusted third parties. The benefit of third-party experts is that it's their full-time priority to stay on top of ever-changing security threats, understand the intricacies of compliance regulations, and have a comprehensive view of the specific security technologies that are needed in each type of environment to prevent unauthorized access and the exposure of sensitive data.

On top of having access to experts, it is in the best interest of every company to have one person on the management team who has oversight responsibility for all IT security as well as for meeting related compliance efforts. Typically, this responsibility is held by a Chief Information Security Officer (CISO), but companies in highly regulated industries may also have a Chief Compliance Officer. In addition to oversight responsibilities, these officers deliver regular status reports to company leadership and fulfill the reporting requirements for regulatory agencies.

**A summary of the specific regulations of 23 NYCRR 500 that correspond to this best practice:**

### 500.04 Chief Information Security Officer

If one doesn't already exist, a Chief Information Security Officer must be appointed who reports to the company's board of directors and oversees and enforces the company's cybersecurity program and policies. Some organizations may choose to use a third party to fill this role.

### 500.10 Cybersecurity Personnel and Intelligence

Designate qualified individuals to manage evolving cybersecurity threats and responses. These individuals can be in-house staff or third-party service providers.

### 500.17 Notices to Superintendent

Covered entities must submit to the New York State DFS an annual written statement, along with supporting documentation, that demonstrates the company is maintaining compliance with the regulations.

# Best practice #3: Regularly Assess Risk and Test Systems for Vulnerabilities

Any comprehensive IT security program requires taking proactive steps that actively seek out and remediate vulnerabilities. This process, known as a security risk assessment, should be performed as part of the development of formal IT policies and plans and then repeated at least once per year thereafter in accordance with established IT policies and plans. In fact, some compliance regulations have numerous requirements that rely on the findings from your risk assessments and 23 NYCRR 500 is no exception.

Risk assessments are typically done with the assistance of a qualified third party in order to maintain an important separation of duties between those who manage or use systems and those who conduct the risk assessment. Although that's not required by 23 NYCRR 500, other compliance regulations do specify that IT risk assessments be conducted by third parties. And speaking of third parties, if you are working with any IT service providers that might have access to sensitive data, it is critical that the activity and access credentials of these entities are included as part of your security risk assessment.

Your risk assessment may include tests that are designed to breach your system defenses, sometimes referred to as penetration tests. If not conducted as part of your risk assessment, then it is beneficial to periodically perform tests that try to find unauthorized routes into your system, particularly into databases where sensitive data is located. A great deal can be learned from such tests.

**A summary of the specific regulations of 23 NYCRR 500 that correspond to this best practice:**

### 500.05 Penetration Testing and Vulnerability Assessments

Financial institutions are expected to perform regular penetration tests of its systems. These tests will be based on known risks that have been identified through the risk assessment.

### 500.09 Risk Assessment

"Covered Entities" are required to conduct a periodic risk assessment in accordance with written policies and procedures and to document the outcome. The resulting documentation should include a description of how identified risks will be mitigated or why they'll be accepted.

# Best practice #4: Implement Technologies and Processes that Prevent Unauthorized System Access and the Exposure of Sensitive Data

There are several important technologies and processes that should be implemented to restrict user access while minimizing the potential of sensitive information being breached. Some of the more common ones include:

- Strong password enforcement—Weak passwords and dormant user profiles pose a significant security vulnerability to organizations. Corporate password policies and system settings that require strong passwords can reduce this risk.
- Elevated authority management—Any IT environment containing sensitive data should strictly limit the number of high-authority user profiles. On IBM i, this includes any profile with *ALLOBJ or *SECADM authority, command-line access, and other potentially dangerous capabilities. For any other user who requires a high level of authority to do a particular job, the requisite authority should be granted only on a temporary basis and within narrowly defined parameters.
- Multi-factor authentication—To strengthen authentication requirements beyond single passwords, numerous regulations require an additional layer of authentication to prevent unauthorized access to sensitive data. Multi-factor authentication technology requires users to provide two or more identifying factors before access is granted. Not only used to control access to systems, multi-factor authentication can usually be implemented to control access to specific databases, commands, and even individual files.
- Access control via networks, open-source functions, and commands—Traditional object-level IBM i security is insufficient for preventing unauthorized access in all circumstances. Rules-based exit programs and other rules-based technologies can put fine-grained controls in place to minimize this threat.
- Encryption and tokenization—Sensitive information in databases can be hidden from unauthorized users when encryption or tokenization technologies are used; the technology that's chosen depends on the use case. Encryption should also be used when sensitive information is stored on backups or save files. And when sensitive files need to be transmitted between partitions, internal systems, or external entities, technologies that support secure file transfer must be used to encrypt this "in-motion" data.

### A summary of the specific regulations of 23 NYCRR 500 that correspond to this best practice:

### 500.07 Access Privileges

Ensure that the proper levels of access are limited to designated personnel who are authorized to access specific systems. Access privileges must be reviewed periodically.

### 500.08 Application Security

Proactively find and fix code vulnerabilities in applications. In some cases, flaws in applications have as much potential for breach as network vulnerabilities.

### 500.12 Multi-Factor Authentication

Whenever authorized users need to access systems that contain sensitive data from an external network, they are required to do so through a multi-factor authentication process.

### 500.15 Encryption of Nonpublic Information

Any information that identifies personal data about individuals must be protected by encryption or by some other means that provides "effective alternative compensating controls reviewed and approved by the Covered Entity's CISO," both when data is at rest and when it's transmitted between systems or entities.

# Best practice #5: Monitor Systems for Cybersecurity Events, Implement Audit Trails, and have an Incident Response Plan

Preventative measures are critical, but equally important are technologies and processes that monitor and log access to sensitive data so that IT managers and security officers can quickly spot unusual activity on systems and take appropriate action.

IBM i provides powerful, unalterable auditing capabilities that utilize the inherent journaling functions of the operating system. When properly configured and enabled, a combination of security-audit and data-object journaling makes it possible to trace and document events related to authentication, system access, data changes, data decryption, configuration changes, and more. In addition, third-party technologies exist that make it possible to keep a record of whenever sensitive data is viewed by a user— regardless of whether the data is changed.

A growing number of companies are utilizing a centralized security information and event management (SIEM) solution to comprehensively collect security event data across systems while providing advanced monitoring and reporting functions. The sophisticated predictive-analytics capabilities that come with many SIEM technologies make it easier for security officers to find patterns that indicate a potential breach.

Finally, in the event a breach is detected, it is invaluable to have an incident-response plan that guides IT staff and management as to the system-lockdown, documentation, and communication protocols that need to be followed. Ideally, the incident-response plan should be included as part of a company's overall IT security plan.

**A summary of the specific regulations of 23 NYCRR 500 that correspond to this best practice:**

### 500.06 Audit Trail

The ability to provide audit trails must be implemented to detect and respond to security events that could materially harm operations. These records are to be kept for five years.

### 500.14 Training and Monitoring

Procedures and controls must be implemented that monitor the activity of authorized users while detecting unauthorized access to or tampering with sensitive data. In addition, companies must provide employees with periodic security training that addresses the risks identified through the company's risk assessment.

### 500.16 Incident Response Plan

Companies must be able to provide a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that could affect the confidentiality, integrity, or availability of systems.

### 500.17 Notices to Superintendent

When it's determined that a breach has occurred, covered companies must provide notice to the New York Department of Financial Services within 72 hours.

# How Precisely Can Help

For companies that are committed to meeting rigorous security best practices, it helps to have a trusted partnership with an organization that can provide essential expertise, technologies, and training. For hundreds of companies around the world, Precisely is that trusted partner, delivering best-in-class security software and services.

## Precisely Security Software for IBM i

Precisely's best-of-breed security software solutions for IBM i help you address access control, protection of sensitive data, audit/trace of security events, and assessment of risk. Security solutions from Precisely encompass:

- System access control
- Database access control
- Encryption, tokenization, and anonymization
- Elevated authority management
- Multi-factor authentication
- Secure file transfer
- System and database monitoring and reporting
- Model-based compliance management
- Security risk assessment
- SIEM integration

Precisely also offers solutions and services for AIX, Windows, and Linux that address security and compliance-auditing needs.

## Precisely Professional Services for IBM i

Our team of IBM i security experts is available to work closely with your staff in numerous ways:

- Ensure a successful implementation of Precisely security technologies and provide all needed training
- Perform in-depth risk assessments on your IBM i environments. Using detailed findings from the assessment, we'll sit down with your IT and compliance managers to help formulate and implement a plan for remediating discovered vulnerabilities.
- Assist your team during compliance or security audits by generating reports required by your auditors
- Provide Managed Security Services that give your company dedicated IBM i security experts who, depending on the level of service chosen, regularly check security configurations, deliver status reports, implement IBM i OS updates and PTFs, monitor your systems 24x7 for security events, adjust security configurations, and assist during compliance or other audits.

To learn more about all of our security products and services, visit www.precisely.com precisely