NY DFS Cybersecurity Compliance

Let our security experts and specialists assist in the design and implementation of a comprehensive strategy to effectively meet NY State Department of Financial Services regulatory standard for Cybersecurity.

Financial services have become a significant target of cybersecurity risks, threats, and vulnerabilities lately. Given this, NY DFS has developed a regulatory standard for cybersecurity. The regulation focuses on protection of customer information and protection of information technology systems of regulated entities. It requires organizations to assess their risk profiles, obtain a security program that addresses these risks, and supply an annual certification confirming compliance.

How AT&T can help:

Whether you are a large firm with existing security or a smaller firm needing to build a security program from the ground up, AT&T Security Consulting experts are available to provide consulting and solutions to strategically assist your business on the road to compliance.

From creating security policies and establishing a virtual CISO to security awareness and training programs, our team is equipped and ready to help facilitate your organization.

- Information security and risk management
- Security operations
- Security response

The New York State Department of Financial Services (NY DFS) has passed a set of regulations (23 NYCRR 500) that went into effect March 1, 2017.

Compliance

NY DFS Regulations

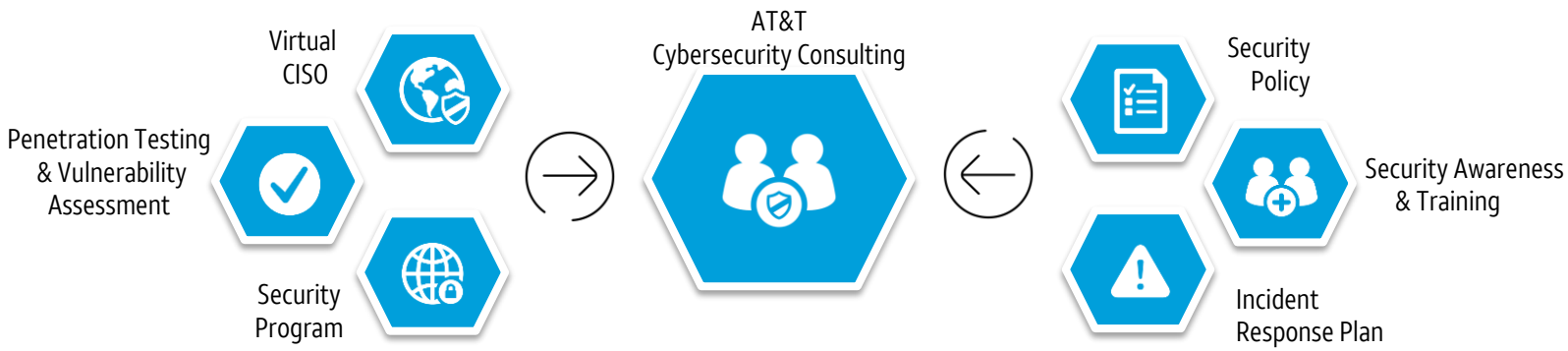
Covered Entity

This compliance calls for Covered Entities supervised by NY DFS to establish and maintain cybersecurity programs.

Contact us to get started with developing a strategy to address your NY DFS security requirements.

AT&T Business

Let our Cybersecurity experts help address your security needs so you can focus on what you do best



Engage the NY DFS standard for your business following these security activities:

6 months

- ***Cybersecurity Program:*** *help protect the confidentiality, integrity, and availability of your firm's information systems*
- ***Cybersecurity Policy:*** *policies set to help protect IT systems and nonpublic information*
- ***Access Privileges:*** *should be limited to your firm's IT systems and nonpublic information, as appropriate*
- ***Cybersecurity Personnel and Intelligence:*** *experts and specialists set to oversee the performance of key security functions*
- ***Incident Response Plan:*** *plan to promptly respond to a security incident and recover any lost information*
- ***Notices to Superintendent:*** *notify NY DFS superintendent in the event of a security incident*

12 months

- ***Chief Information Security Officer:*** *CISO must be in place to report an incident to the firm's board of directors or senior officers*
- ***Penetration Testing and Vulnerability Assessments:*** *annual penetration test and bi-annual vulnerability assessments*
- ***Risk Assessment:*** *conduct a security risk assessment on IT systems and nonpublic information and update as necessary*
- ***Multi-Factor Authentication:*** *these methods must be used to access internal networks from an external network*
- ***Training and Monitoring:*** *provide regular security awareness training to employees*
- ***Incident Notices to Superintendent:*** *submit a written statement to the NY DFS superintendent to verify your compliance with NY DFS cybersecurity requirements by February 15th of each year*

18 months

- ***Audit Trail:*** *maintain security systems that can log and reconstruct material financial transactions for the purpose of detecting and responding to incidents*
- ***Application Security:*** *establish written procedures and guidelines for the highly secure development, monitoring, and assessment of applications created in-house*
- ***Limitations on Data Retention:*** *establish policies and procedures for securely disposing of nonpublic information*
- ***Training and Monitoring:*** *risk-based policies and procedures to help detect unauthorized access of nonpublic information*
- ***Encryption of Nonpublic Information:*** *encrypt nonpublic information while at rest and in transit over external networks*

24 months

- ***Third Party Service Provider:*** *develop written policies to see to it that nonpublic information is highly secure when shared with third-party service providers*

The timelines and the activities outlined here are a high level overview and should not be treated as a comprehensive list of actions.

Exemptions: Companies with fewer than ten employees, less than $5M in revenue over the last 3 years, or less than $10M in total assets. Appropriate exemption forms must be filed with NY DFS.

AT&T Business