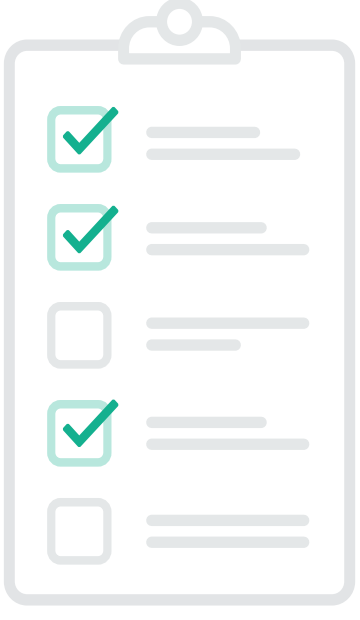
STOP FREAKING OUT.

VERA

A short, simple guide to tackle the New York Department of Financial Services' Cyber Regulations



MORE CYBER REGULATIONS?

You're already subject to oversight from multiple authorities, monitoring a mesh of requirements at the federal, state and local level. You need a consistent way to address them all, and you need to choose investments that will reduce operational costs, optimize compliance resources, cut process, and eliminate last minute scrambling and frankly, head-aches.

WE GET IT.

We're here not only to help you navigate the newest set of cybersecurity regulations coming your way, but to help you adopt an approach that scales in the face of future cybersecurity requirements.

OUR GOAL WITH THIS GUIDE IS SIMPLE AND TWO-FOLD:

1. Break down the New York Department of Financial Services' ("NY DFS") proposed new cybersecurity rules, which took effect on March 1st, 2017; and

2. Share why Dynamic Data Protection is the simple, go-to solution to tackle the new requirements, and make sure you protect and control access to your team's highly sensitive data, everywhere. Seriously, everywhere.

A CLEAR FOCUS ON DATA IN NEW YORK'S "FIRST-IN-THE-NATION" CYBER REGULATIONS

In September 2016, Governor Cuomo and the NY DFS announced "first-in-the-nation" rules strengthening cybersecurity requirements for financial firms in the state of New York.

The breadth of covered entities is broad, and the regulations are aimed at protecting consumers and the financial system from cyber threats. Banks, insurers and financial institutions regulated in New York will be subject to the new rules, which became effective on March 1st, 2017. Covered entities will be required to have a cybersecurity program in place by August 28, 2017 and begin filing the annual compliance certification on February 15, 2018.

"New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm that is often perpetrated by state sponsored organizations, global terrorist networks, and other criminal enterprises."

— ANDREW CUOMO, GOVERNOR OF NEW YORK

WHAT'S NEW? BROAD ENCRYPTION, AUDIT TRAILS AND A REMOTE CONTROL FOR YOUR DATA

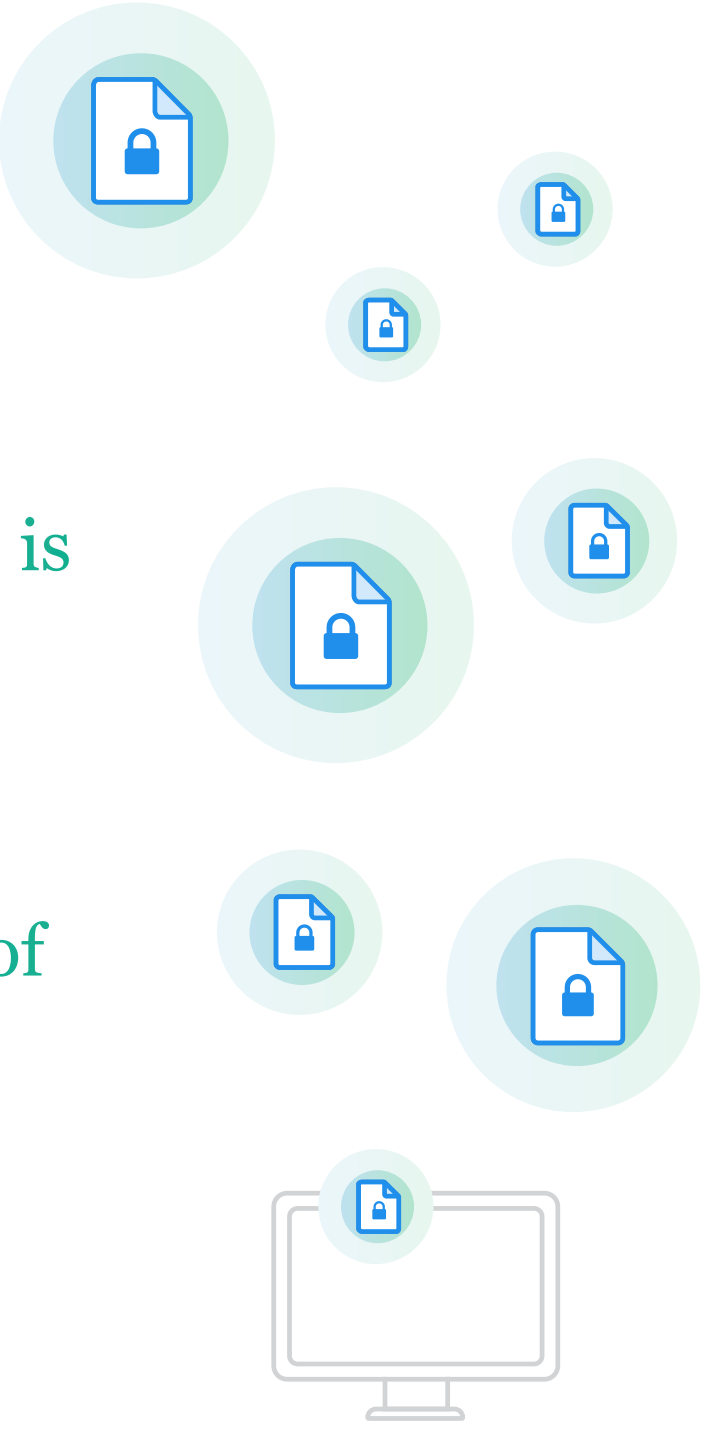
You're likely already implementing a Cybersecurity Program that identifies, protects and responds to cyber security events, and are layering the supporting policies and procedures. But, the new NY DFS regulations are different in one major respect, and this is a significant departure from past work.
The new rules are focused not just on protecting information systems but on securing, auditing and the disposition of data itself.

Firms not only need to dramatically expand the categories of data to encrypt (the draft calls for the "encryption of all nonpublic information held or transmitted"), they'll also need to tie it to access control (enforce who can and cannot access a specific file), define acceptable usage policies (what rights an individual should or should not have with the information), increase auditability (track the life cycle and all access points to nonpublic information), and enforce data retention (plan for the preservation and timely disposition of nonpublic information).

THE DATA-CENTRIC ADDITIONS ARE CAPTURED IN FOUR KEY CLAUSES IN THE PROPOSAL:

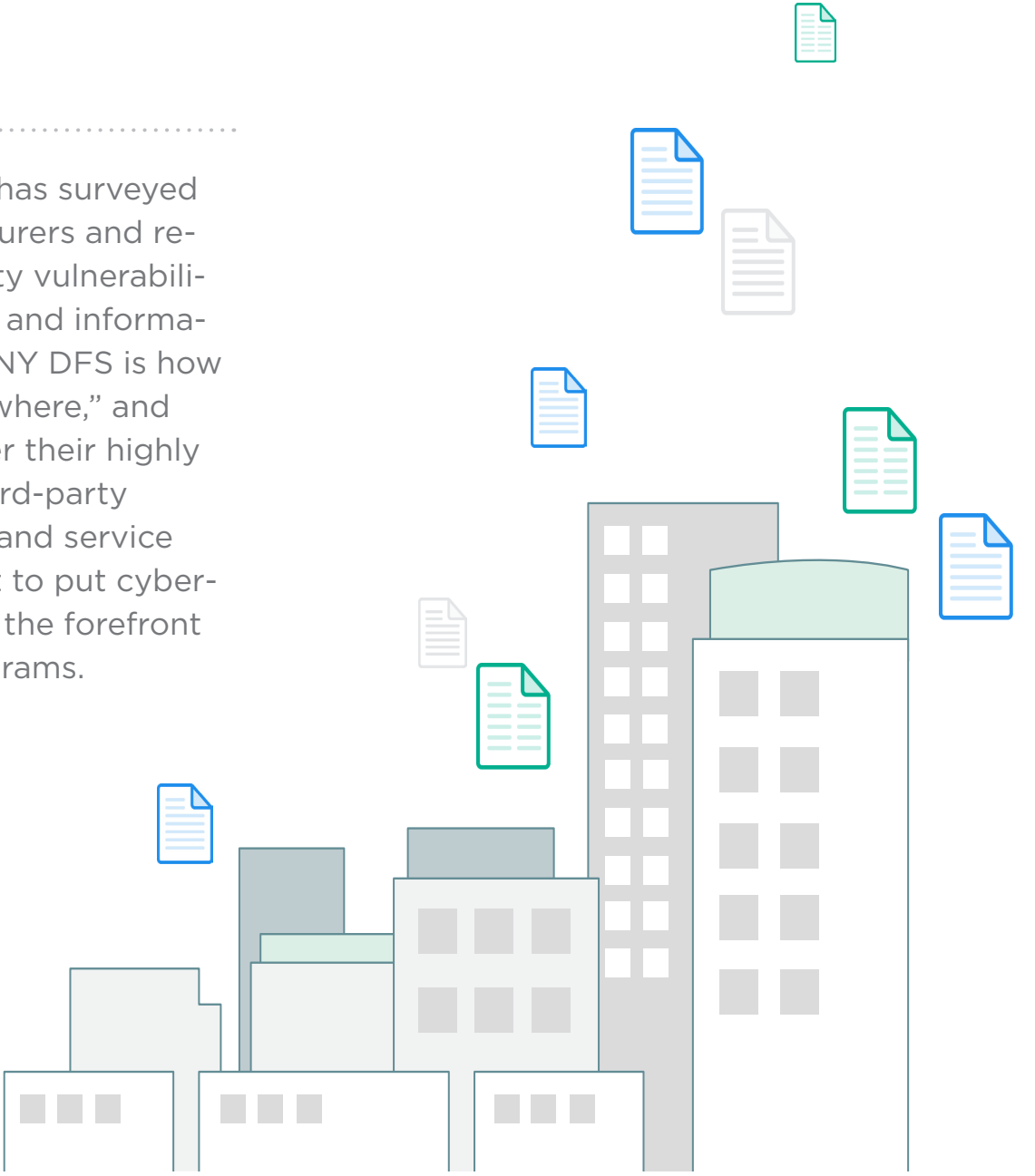
- **Encrypt** all "nonpublic information held or transmitted" in the firm
- **Restrict access privileges** not only to systems but to the data itself
- **Implement an audit trail** system to reconstruct transactions and log access privileges
- Provide for the **retention and "timely destruction"** of non-public information

"But, the new NY DFS regulations are different in one major respect, and this is a significant departure from past work. The new rules are focused not just on protecting information systems but on securing, auditing and the disposition of data itself."



WHY IS THIS HAPPENING? SHARING AND THE 'DATA EVERYWHERE' PROBLEM.

Over the past several years, the NY DFS has surveyed close to 200 banking institutions and insurers and reported "significant potential cybersecurity vulnerabilities" in financial firms' private client data and information systems. A big driving force for the NY DFS is how often client information is shared "everywhere," and how little control financial firms have over their highly sensitive data once shared with these third-party service providers (e.g., lawyers, auditors and service providers). Tighter regulations are meant to put cybersecurity - data-centric cybersecurity - at the forefront of every financial firm's agenda and programs.



LET'S CUT TO THE CHASE. SIMPLE ENCRYPTION WON'T BE ENOUGH TO COMPLY WITH THE NY DFS REGULATIONS.

The data-centric nature of these requirements presents a bit of a curveball to security and risk teams. To comply, firms will have to implement protections beyond simple encryption at rest and in transit.

Why? Encryption at rest and in transit only protects data while it's exchanged between two trusted parties. But simple encryption cannot scale to meet the enhanced NY DFS requirements. It doesn't limit access rights, provide an audit trail of data governance in and outside the firewall, or remotely dispose or enforce the timely destruction of records and other information.

Current strategies for security and compliance won't cut it - we need a different approach altogether. Instead of layering multiple tools, you need a single solution that can help you meet the increased data security mandate.

That's why financial firms of all sizes need Dynamic Data Protection. It's a better model for protecting data in a connected economy, and the only way to meet all the data-centric protection requirements established by the NY DFS.

WHAT IS DYNAMIC DATA PROTECTION?

Vera's Dynamic Data Protection platform is the intelligent, seamless and proactive solution financial firms leverage to secure all corporate data through its entire life cycle.

Unlike simple encryption, Vera's Dynamic Data Protection cannot be stripped off the file the moment it's downloaded or opened by the recipient. Your team is empowered to always enforce your firm's security controls and usage policies on highly sensitive files, even after data is shared outside the firm, downloaded, duplicated or moved to unmanaged domains.

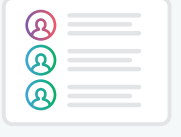
In the event of a breach, whether from an outside actor, intentional misuse, insider negligence, or just smart people making the rare dumb mistake, Vera gives you the tools to update or revoke access, instantly, to all copies of the file or specific users or vendors.

WITH VERA, YOU CAN CONTROL:

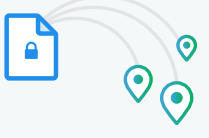
WHO
Who has access to your files

WHAT
What they can/cannot do with them (e.g., edit, view only, watermark rights)

FOR HOW LONG
For how long collaborators can access (e.g., automatic time expiration, retention rules, granular revoke access capabilities)



AUDIT
Audit all authorized (and unauthorized access) attempts with a full audit trail



ANYWHERE YOUR DATA TRAVELS

HERE ARE FOUR WAYS VERA'S DYNAMIC DATA PROTECTION HELPS YOU MEET THE NY DFS DATA SECURITY GUIDELINES:

1

ENCRYPT ALL "NONPUBLIC INFORMATION HELD OR TRANSMITTED" IN THE FIRM

Simple encryption doesn't scale when the NY DFS requires encryption and data loss protection not only to records at rest, but anywhere your data "is transmitted." Vera encrypts your data with strong AES-256 encryption, and goes further to prevent unwanted viewers to your information anywhere that information moves, and applies data-in-use protections that control and limit what recipients can/cannot do with your firm's nonpublic information.

HOW IT WORKS:

A leading New York hedge fund with over $20 billion in assets under management uses Vera to automatically encrypt and secure all confidential email attachments transmitted beyond the fund. Vera ensures that only valid email recipients can access the fund's private information. Vera also enforces the firm's security policies, giving third-party service providers, for example, view-only rights and prohibiting them from printing, modifying or copying sensitive information out of the document, anywhere that document is moved.

TIP:

Leverage Vera to automate encryption for data at rest in any of your content repositories on-premises or in the cloud (e.g., SMB, local folders, Box, Dropbox, and more) or automatically secure information transmitted beyond your firm (via email or shared link from tools like Box and Dropbox).

2

RESTRICT ACCESS PRIVILEGES NOT ONLY TO SYSTEMS BUT TO THE DATA ITSELF

In a complex technology ecosystem, it's no longer feasible to define access at the system, device, or perimeter level. When you define identity exclusively at the system level, employees and third-party providers have unfettered access to anything stored in those systems, and once they remove those files, they're gone. Vera defines and restricts access privileges at the file level, helping your team maintain those strict data governance requirements anywhere files travel.

Think of Vera as enforcing a guest list on each piece of your nonpublic content. Only approved parties can access your nonpublic information, no matter where that file is stored, where it travels or if it's forwarded.

HOW IT WORKS:

An influential asset manager in Manhattan utilizes Vera to automatically secure all legal, HR, and financial data stored in its local file shares. Vera integrates with the fund's Active Directory to assign rights and permissions to highly sensitive data. For example, Finance team members in the folder have different rights than Legal team members. Now, even if the file is removed from the drive, the access privileges the fund designated stick to the file, anywhere it goes.

TIP:

Vera natively integrates with cloud collaboration tools, including Box and Dropbox, enforcing rights and permissions to your confidential content in the cloud and beyond.

3

IMPLEMENT AN AUDIT TRAIL TO RECONSTRUCT TRANSACTIONS AND LOG ACCESS PRIVILEGES

In the past, the requirement for an audit trail on data access was seen as an add-on or an after-thought. With the NY DFS requirements calling for improved visibility into data use, you need an automated way to track and log access privileges and reconstruct transactions. Luckily, Vera provides granular 360-degree visibility into all access attempts of your nonpublic information (both authorized and unauthorized attempts) with a full audit trail of who, where, and how your firm's data was accessed to help you build a better picture of your data use.

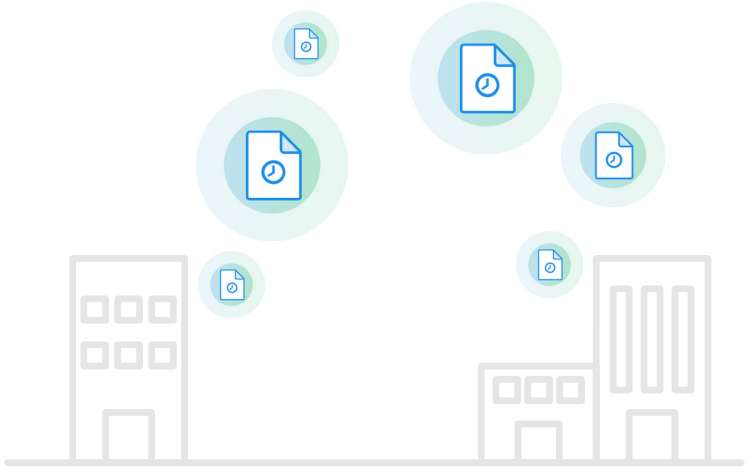
HOW IT WORKS:

A private equity (PE) shop in New York leverages Vera to track quarterly letters sent to its limited partners (LPs). With Vera, the PE fund has a full audit log of how, when and whether their LPs opened their investor communications, and can even track whether competitors or non-accredited investors have attempted to access its nonpublic information. In the event of an audit, the PE shop has a complete audit log and picture of access privileges, access attempts and the life cycle of its non-public information.

TIP:

Export Vera's audit log into your favorite SIEM/BI tools for further monitoring and detailed analysis.

4



PROVIDE FOR THE RETENTION AND "TIMELY DESTRUCTION" OF NON-PUBLIC INFORMATION

Simple encryption and common security tools like Data Loss Prevention (DLP) cannot remotely destroy nonpublic information once it's sent beyond the firm. Vera gives you control of your data through its entire life cycle, as it moves beyond your systems, through the proverbial "last mile" to another partner's desktop, phone, or cloud application. It offers flexible, customizable policies, including the ability to:

- **Automatically expire information after a defined period;**
- **Easily create rules that provide for data retention; and**
- **Revoke access to any user, at any time, at the click of a button**

HOW IT WORKS:

The mergers and acquisitions arm of a public banking entity leverages Vera to remotely destroy its nonpublic information after the bank's retention period expires. Access to all copies of the diligence materials, investor decks, financial models, accounting profiles, and audits are automatically destroyed, even if they've been moved to personal devices or unmanaged domains. The bank's security team now has peace of mind that its retention and record disposition rules are enforced, everywhere.

TIP:

Leverage Vera to instantly revoke access to information, if an employee accidentally sent out the wrong file to the wrong person. You can lock down the entire file or specific users. Then, check Vera's audit log to track whether that file was ever accessed to get a complete picture of your liability.

CONCLUSION

New York's "first-in-the-nation" regulations signal one thing: protecting the perimeter and your information systems alone won't cut it to meet the enhanced NY DFS data security requirements. It's clear firms will need to deploy a data-centric strategy with dynamic forms of data protection that extend beyond their current systems.

The good news: these proposed regulations will not only reduce the risk of external attacks for your firm, they'll also dramatically reduce the risk of data breaches from insider threats, negligence, and the unintentional misuse of data.

Even more good news: Vera's Dynamic Data Protection is your simple, seamless go-to solution to help your team meet the enhanced data security requirements and scale in the face of future cybersecurity requirements.

Ready to see Dynamic Data Protection in action?

Visit us at www.vera.com, and check out these other helpful resources:

- **Tackling NY Cyber Regulations: Encryption Isn't Enough**
- **Regulation: New York Department of Financial Services Regulations Proposed Cybersecurity Requirements for Financial Companies (September 13, 2016)**
- **Press Release (September 13, 2016): Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions**

318 Cambridge Ave
Palo Alto, CA 94306

sales@vera.com
Vera HQ
@VeraSecurity