23 NYCRR 500 Whitepaper

For Customers Licensed in the State of New York

Submitted by: Matthew R. Johnson, JD
Associate Legal Counsel
Employee Pooling, LLC
615-610-5585 (ex. 204)
matthew@employeepooling.com
https://www.employeepooling.com

Harmeet Singh
Chief Operating Officer and Head of Data Security
Employee Pooling Resources, Pvt. Ltd.
615-610-5585 (ex. 301)
harmeet@epr-india.com

Employee Pooling, LLC (USA):
2000 Glen Echo Rd,
Suite 111
Nashville, TN 37205
615-610-5585 (ex. 204)
info@employeepooling.com

Employee Pooling Resources Pvt. Ltd. (India):
B – 54 New Krishna Park, Vikaspuri,
New Delhi, India – 110018
From India: 987-150-2546
From US: 615-610-5585 (ex. 301)

Table of Contents

Executive Summary

Employee Pooling, LLC (d/b/a Employee Pooling and "EP") has been organized and doing business since February 2011 as a round-the-clock processing center for insurance agencies and mortgage businesses. As an offshoring business, EP is made up of two offices. The home, administrative office is in Nashville, Tennessee. The other office, Employee Pooling Resources, Pvt. Ltd. ("EPR"), is a separate unincorporated entity located in Delhi, India that is owned by EP. These businesses are hereby together referred to as "EP" in this document unless stated otherwise.

The State of New York drafted Regulation 500 ("23 NYCRR 500" or "the Regulation") as a part of its state law, the New York Codes, Rules and Regulations, and codified it in Title 23 (Financial Services) to protect consumer information and the information technology systems of certain regulated financial entities licensed or doing business in New York. 23 NYCRR 500 became effective March 1, 2017 and applies to entities "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law" of the State of New York.[1] There are some exemptions for smaller businesses, and penalties and sanctions for failure to meet and retain most provisions laid out in the Regulation.

EP must handle sensitive, personally identifiable information, including occasionally handling Protected Health Information ("PHI") as defined in the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 and its related regulations, to perform services for its customers. EP acknowledges the extreme importance of maintaining the integrity and privacy of client information, including information belonging to clients who fall within 23 NCYRR 500. As such, EP makes administrative, physical, and technical safeguards a priority in all its business dealings to protect client information.

In recognition of the adoption of 23 NYCRR 500, EP provides this package as a general whitepaper for its prospective and current customers that are operating or have a license to do business in New York and to demonstrate EP's dedication to a highly secure environment to protect information. EP is always evaluating its current security processes, and this document will be expanded in scope moving forward to reflect evolving technology, laws, and business practices.

Note that capitalized words not defined in this whitepaper have the same definition or meaning as they have in 23 NYCRR 500.

The information contained in this whitepaper is provided for informational purposes only and should not be construed as legal advice on any subject matter. **You should consult with an attorney and/or security professional before taking action on any matter described herein**.

[1] 23 NYCRR 500.01(c)

About 23 NYCRR 500

A. *General*

The State of New York drafted Regulation 500 ("23 NYCRR 500") as a part of its state law, the New York Codes, Rules and Regulations, and codified it in Title 23 (Financial Services) to protect consumer information and the information technology systems of certain regulated financial entities licensed or doing business in New York. 23 NYCRR 500 became effective March 1, 2017.

The entities required to comply with 23 NYCRR 500 are called "Covered Entities". Covered Entities are individuals or non-government business entities that "operat[e] under or [are] required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law".[2] While applicable individuals, agencies and businesses located within the state of New York are clearly required to comply with 23 NYCRR 500, Covered Entities that exist *outside* of New York must also comply; note the criteria are simply that Covered Entities have or should have a license, registration, *etc*. in New York. Therefore, an insurance agency located in Texas licensed to sell insurance in New York is covered by this law and could be prosecuted or held responsible for breaches despite being located in another state.

To this end, Covered Entities are required "to assess [their] specific risk profile and design a program that addresses [their] risks in a robust fashion,"[3] meaning that they must develop certain procedures to protect consumer information and "maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems."[4] Absent certain exemptions described below, the specific requirements that Covered Entities must implement under the Regulation are the following:

1. **Cybersecurity Program**: Components of Covered Entities' cyber security programs are laid out in 23 NYCRR 500.02.
2. **Cybersecurity Policy**: Covered Entities must maintain and implement a cybersecurity policy. Particular elements of the cybersecurity policy are described in 23 NYCCR 500.03. A "Cybersecurity Policy" contrasts from a "Cybersecurity Program" in that the former are written policies designed to enhance the framework of the latter.
3. **Chief Information Security Officer ("CISO") and Cybersecurity Personnel**: Covered Entities must designate a qualified individual responsible for overseeing and implementing the Covered Entity's Cybersecurity Program. The CISO may be employed by the Covered Entity *or may be from a Third-Party Service Provider*, but all potential CISOs must fulfill the requirements laid out in 23 NYCCR 500.04. Covered entities must also utilize qualified cybersecurity personnel who can manage cybersecurity risks and can provide training and updates to address cybersecurity risks. 23 NYCCR 500.10.
4. **Penetration Testing**: Covered Entities' cybersecurity programs must test for vulnerability of its security systems. 23 NYCCR 500.05.
5. **Audit Trails**: Covered Entities' cybersecurity programs must maintain records, or audit trails, that permit it to reconstruct operations and financial transactions should a breach occur; permit it to detect and respond to breaches that have a likelihood of materially

[2] 23 NYCRR 500.01(c).
[3] 23 NYCCR 500.00.
[4] 23 NYCRR 500.02(a).

harming the Covered Entity; and keep the records for 3-5 years, depending on the record type. 23 NYCRR 500.06.

6. **Review Access Privileges to Covered Entities' Nonpublic Information**. Covered Entities must limit its users' access privileges to its Information Systems that provide access to Nonpublic Information and periodically review such access privileges. 23 NYCRR 500.07.
7. **Write procedures and security guidelines for in-house developed applications used by the Covered Entity**. 23 NYCRR 500.08.
8. **Risk Assessment**: Covered Entities must conduct periodic risk assessments of their Cybersecurity Program as changes in their business environment and evolutions in technology occur. 23 NYCRR 500.09.
9. **Multifactor Authentication ("MFA")**. MFA is Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism; *e.g.*, a text verification sent to your phone after logging into some software. Covered Entities must enable MFA on relevant computers, internal networks, software systems to protect against unauthorized access to Nonpublic Information or Information Systems. 23 NYCRR 500.12.
10. **Secure Disposal of Secure Information**. Covered Entities must develop policies and procedures and follow them for the secure disposal of any Nonpublic Information that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible. 23 NYCRR 500.13.
11. **Training and Monitoring**. Covered Entities must provide regular cybersecurity awareness training for all personnel that is updated to reflect current risks and implement policies to monitor the activity of Authorized Users who have access to Nonpublic Information. 23 NYCRR 500.14.
12. **Encryption Procedures**. Covered Entities' CISO and their staff must determine and approve encryption mechanisms on applicable software and systems to protect the access of Nonpublic Information.[5] 23 NYCRR 500.15.
13. **Incident Response Plan**. Covered Entities must "establish a written incident response plan designed to promptly respond to, and recover from, any [breach] materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations". 23 NYCRR 500.16.

[5] 23 NYCRR 500.15(a)(1).

B. *Exemptions*

Not all Covered Entities must comply with every section laid out in the Regulation. Section 500.19(a) of the Regulation contains the following types of individuals or business entities that are exempted on a limited basis:

1. Covered Entities with fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, **or**
2. Covered Entities with less than $5,000,000 in gross annual revenue in each of the last three (3) fiscal years from New York business operations of the Covered Entity and its Affiliates, **or**
3. Covered Entities with less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates.

If your business or agency falls in any one of these three categories, then it is exempt from the requirements Regulation Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16. These specific sections are described in further detail above.

Section 500.19(a) provides the major exemptions. Other limited exemptions are stated within Section 500.19.

If your business or agency believes it is exempt, consult with a professional. Any Covered Entity that qualifies an exemption must file a "Notice of Exemption" within 30 days of the determination that the Covered Entity is exempt.

An example of a Notice of Exemption is contained on page 14 of this whitepaper.

Application of 23 NYCRR 500 to Employee Pooling

Third-Party Service Providers (like EP) are also addressed in the Regulation. An "Authorized User" under the Regulation may be an agent or contractor from a Third-Party Service Provider or an employee of the Covered Entity or an Affiliate.[6]

23 NYCRR 500 puts the primary burden on Covered Entities. Covered Entities should audit its Third-Party Service Providers and fill out a "Certification of Compliance" following a successful audit and review of its information systems and security practices. The purpose of the "Certification of Compliance" is for Covered Entities themselves to complete and submit annually starting February 15, 2018.[7]

A Third-Party Service Provider cannot and should not fulfill adequate due diligence under the Regulation for a Covered Entity simply by providing it with a written statement saying "we comply," *e.g.*, EP simply providing evidence of a "Certification of Compliance" required under the Regulation.[8] While providing a Certification of Compliance may be a factor to consider for due diligence purposes, it alone is not sufficient.

Rather, Covered Entities "must assess the risks each Third-Party Service Provider poses to their data and systems and effectively address those risks."[9] This means ensuring the Third-Party Service Provider fulfills necessary applicable requirements stated on pages 3 – 4 of this whitepaper above. When the Covered Entity signs its Certification of Compliance, it is effectively stating that it has reviewed all its internal security policies, and those of its Third-Party Service Providers, and is saying it and the Service Provider are compliant. The Third-Party Service Provider's cybersecurity policy must be based on the Covered Entities' risk assessment as described in 23 NYCRR 500.09.[10]

To that end, if your agency or business is a Covered Entity under the Regulation, we invite your agency's or business' team to discuss any security concerns with us and send us appropriate security questionnaires and audit forms so we can assist your team in maintaining compliance under the Regulation. While we can provide your agency or business with the necessary evidence and demonstrate that we maintain industry-accepted security practices, the Regulations provide your team should first assess our practices and then annually complete the Certification of Compliance to maintain compliance under the Regulation.

An example of a Certification of Compliance is provided in this document on page 13.

The remainder of the documentation in this whitepaper describes some of the security practices we have in place and demonstrates compliance with a relevant ISO 27001 certificate.

---

[6] 23 NYCCR 500.01(b).
[7] 23 NYCCR 500.17(b).
[8] http://www.dfs.ny.gov/about/cybersecurity_faqs.htm, Question #2. Appendix A of the Regulation contains a "Certification of Compliance" that a Senior Officer of the Covered Entity must sign annually to fulfill compliance.
[9] http://www.dfs.ny.gov/about/cybersecurity_faqs.htm
[10] 23 NYCCR 500.11(a).

Employee Pooling Resources Security Overview

Employee Pooling
MAXIMIZING HUMAN CAPITAL

Employee Pooling Information Security Overview

Employees:
- NDA
- Background checks
- Physical access restricted to critical areas
- Random physical searches

Physical Security:
- Access control – entry & exit
- Login by password only
- USB ports blocked
- No floppy, CD ROM drives
- All files stored in file server

Network:
- Websites restricted
- Ports opened only with authorization of Head IT
- Quick Heal Total Security for virus and spam control
- Firewall Protection

Process Audits:
- Quality Audits
- Process walk through
- Basic hygiene checks
- Proper training schedule

Emails:
- Web access limited only to authorized users
- Attachment size restrictions
- Unique outgoing and incoming mail servers
- Access only to authorized sites and Content management through Security Software

Business Continuity Process:
- Back up strategy in place
- Offsite storage of back up media
- Leaders trained on emergency response and fire safety drills
- Regular data back-ups

Printing:
- Common network printer
- Physical security to check papers
- Restricted printer access
- Shredder for disposal

EP Security Policies:
- Information Security Policy
- Physical Security Policy
- Data Privacy Policy
- Password Management Policy
- Back Up Policy
- Business Continuity Management
- Clear desk and clear screen Policy

Employee Pooling Resources Security Brief

Physical Security Features

- ✓ EPR owns and uses power generators to continue work during power outages and failures.
- ✓ Employees are not allowed to use writing utensils of any kind while in the office. No writing utensils or paper are on employee desks or near workstations.
- ✓ Employees do not have access to printing devices of any kind. Management exclusively has access to the only common network printer.
- ✓ Physical access to the office is restricted by swipe cards. This access is provided to monitor and control entry and exit of employees as well as other persons.
- ✓ Employees are not allowed to keep their mobile phones or bags with them. Cell phones, purses, and any other personal items must be left in a locker while they are at their desks.
- ✓ Employees are not allowed to carry anything in or out of the office.
- ✓ Background checks are completed on each employee before hiring.
- ✓ EPR uses a shredder to dispose of all papers that contains or may contain personal or sensitive information.
- ✓ Random physical searches of employees' person and workstations are routinely done.
- ✓ The main room containing server, CCTV feeds, and computer control equipment is kept in a locked room inaccessible to employees.

Technical and Electronic Security Features

- ✓ **CCTV cameras are in position to capture each and every activity of employees**. Management is constantly monitoring camera feeds.
- ✓ Recordings from the CCTV cameras are kept for at least 6 months.
- ✓ USB ports on all employee computers and laptops are blocked to prevent data theft or misuse.
- ✓ No CD burners or other type of media that would allow those with access to workstations to copy and remove data from our facility.
- ✓ FileZilla, a file transfer protocol application, is used for secure file sharing between the employees and the office IT management.
- ✓ Management changes all passwords for FileZilla every 90 days.
- ✓ Data shared through Filezilla is encrypted (128-bit encryption) during file sharing.
- ✓ All employees use only a wired CAT-6 Internet connection. Wi-fi connections are not used unless on special occasions, and only then by upper management upon an e-mail sent in advance to IT management.
- ✓ Social media and any type of messenger applications are prohibited and blocked, except where such social media applications are required to be utilized as a part of a contract to perform services. Any type of messenger software included on employee laptops have been uninstalled.
- ✓ EPR utilizes a parental control software, a "keylogger" application, on each system to monitor day-to-day activities of the employees on the system.
- ✓ EPR severely restricts Internet access and only allows our team to access websites that EP management deems necessary, as required for providing its services. All web traffic is restricted by a digital and physical firewall and monitored regularly.

- ✓ Documents are shared and transferred via Citrix ShareFile unless the customer insists on their own file sharing method. ShareFile is both HIPAA and HITECH compliant. EP's information is stored on HIPAA-dedicated servers, and EP has executed a Business Associate Agreement ("BAA") with Citrix ShareFile. More information can be found at the website: https://www.sharefile.com/
- ✓ All incoming and outgoing e-mails which are received or sent by the employees are monitored.
- ✓ Outgoing e-mails are restricted to specific domains (*e.g.*: no allowing outgoing mails to personal e-mails like Yahoo! or G-mail, *etc*.).
- ✓ EPR uses a professional e-mail hosting service which provides unique incoming and outgoing e-mail servers to prevent any risk of misusing e-mails.
- ✓ Administrators have the ability to and implement shadowing employees' work sessions to monitor activity.
- ✓ Employees are required to keep any sensitive data file on system's desktop. The employees' laptops are audited to confirm this restriction.
- ✓ All login information is controlled by the team Manager in India. The manager will log-on users each morning to the accounts they need to access to complete their work for the day.
- ✓ All workstations (approx. 130) are checked once a month to maintain the security level of the systems.
- ✓ Administrative privilege hierarchies are in place. All employees work as "Standard Users" on respective workstations, not having access to full administrative privileges. Installations of any unauthorized software or application are prohibited and prevented.
- ✓ A virtual support portal is in place to maintain a record of errors that occur on the system and steps that are taken to resolve any issues.
- ✓ Data is backed up routinely. EPR management implements proper back-ups in two different drives which are stored within the office and in a location outside the office as well.
- ✓ Virtual registers are maintained to record assets going out and coming in.
- ✓ Employees use dual monitors to work for efficiency and accuracy.
- ✓ EPR recommends its customers to provide it with unique and restricted usernames and passwords to their accounts.
- ✓ Password policy to login into workstations are in place; passwords for workstations change every 90 days.
- ✓ Optimization of each system is scheduled on monthly basis.
- ✓ Proper anti-malware applications are used to protect all computer systems.

Administrative Safeguards and Employee Safety Features

- ✓ EPR has a policy of "clear desk and clear screen." Employees must logout of workstations when they are not present at workstations.
- ✓ Laptops are owned by Employee Pooling. No personal devices are used for work in our facility.
- ✓ All employees have signed non-disclosure agreements.
- ✓ HIPPA and privacy law training is periodically given to each and every employee and upon hiring all employees to make them aware of best practices and the implications of misusing data.

- ✓ Company leaders are trained on emergency response and fire safety drills.
- ✓ The office contains all the amenities an office in the U.S. has, including air-conditioning.
- ✓ Fire extinguishers and first aid kits are kept in the office.
- ✓ Cell phones, recording devices, and any other communication media are prohibited while employees are on the work floor.
- ✓ Management changes all passwords every 90 days for all devices.
- ✓ Data retention and deletion policies are clearly defined.
- ✓ EPR runs a proper attendance system utilizing biometric data to track the time of working hours of each employee.
- ✓ EPR employs a security guard with a metal detector at the main entrance of office premises who keeps all the records for each visitor.
- ✓ EPR implements protocols for guests that visit the EPR office. All guests are required to go through a security checkpoint at the main security counter and are instructed to wait in separate waiting area until the guest can be escorted by EPR management.
- ✓ EPR company policy prohibits any alteration of customers' files or documents.
- ✓ EPR has a privacy liability insurance policy with Allied World Assurance Company that covers privacy and network security, notification and credit monitoring, crisis management, and data forensics. In case of breach, EPR is to contact its insurance provider who will provide it with immediate and ongoing instructions.
- ✓ If any employee is absent, no other EPR employee is allowed to use the absent employee's workstation without permission from IT management.
- ✓ Employees are not allowed to keep any important, sensitive, or personal data on their workstations.
- ✓ EPR has implemented a monitoring system, both online and offline. All systems are put under online as well as offline monitoring systems before handing out to the employees to work.
- ✓ EPR has implemented monitoring systems for network monitoring. EPR receives two kinds of feedbacks from this monitoring:
    - Real time monitoring.
    - Time lapse (every two hours) monitoring.

ISO/IEC 20071:2013 Certificate and Information

The International Standards Organization ("ISO") / International Electrotechnical Commission ("IEC") is a joint standardization subcommittee of the ISO who publishes the ISO/IEC 27001 information security standard, among other standards.

The ISO/IEC 27001 certification demonstrates standards for information technology, security techniques, and information security management systems. The last revision of ISO/IEC 27001 standards were in 2013; hence, the latest standard is titled "ISO/IEC 20071:2013."

EP has attained ISO/IEC 20071:2013 certification. The audit for EP's current certificate was performed by KBN Certification System, a leading quality management company in India which is accredited by the Scotland Accreditation Forum ("SAF"). EP proudly demonstrates its dedication to information security and privacy by providing all prospective customers a copy of its ISO/IEC 20071:2013 certificate.

(ISO/IEC 20071:2013 certificate is on the following page)

Certificate of Registration

This is to certify that

EMPLOYEE POOLING RESOURCES PVT. LTD.

WORK PLACE:- B- 54, KRISHNA PARK, VIKASPURI, NEW DELHI
NEW DELHI- 110059. INDIA.

has been assessed and Certified by KBN Certification System

As Meeting The Requirements Of:

ISO / IEC 27001:2013

Information Security Management System

For the following scope of activities:

BACKEND SERVICES PROVIDER

Date of Registration : 07/02/2018
Re-certification Due : 06/02/2021

1st Survillance Date : 06/02/2019
2nd Surveillance Date : 06/02/2020

Certificate No:- 1322090218

To verify this certificate please visit at www.kbncertification.com

Authorised Signatory

KBN Certification System

MEMBER OF QUALITY COUNCIL OF INDIA

Validity of this Certificate is Subject to annual Surveillance audits done successfully

this certificate of Registration remains the property of KBN Certification System and shall be returned immediately Upon request

Email:- info@kbncertification.com Website:- www.kbncertification.com
D-176, Nawada Housing Complex, Dwarka More, Uttam Nagar,
New Delhi-110059. (INDIA) | Contact No. :- 7551110651

_____

(Covered Entity Name)

February 15, 20_____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of_____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended__(year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date: _____

[DFS Portal Filing Instructions]

APPENDIX B (Part 500)

_____

(Covered Entity Name)

(Date)_____

Notice of Exemption

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- ☐ Section 500.19(a)(1)
- ☐ Section 500.19(a)(2)
- ☐ Section 500.19(a)(3)
- ☐ Section 500.19(b)
- ☐ Section 500.19(c)
- ☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_____ Date: _____

(Title)

(Covered Entity Name)

[DFS Portal Filing Instructions]