Employee Pooling®

MAXIMIZING HUMAN CAPITAL

Security Package – Brief Intro

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

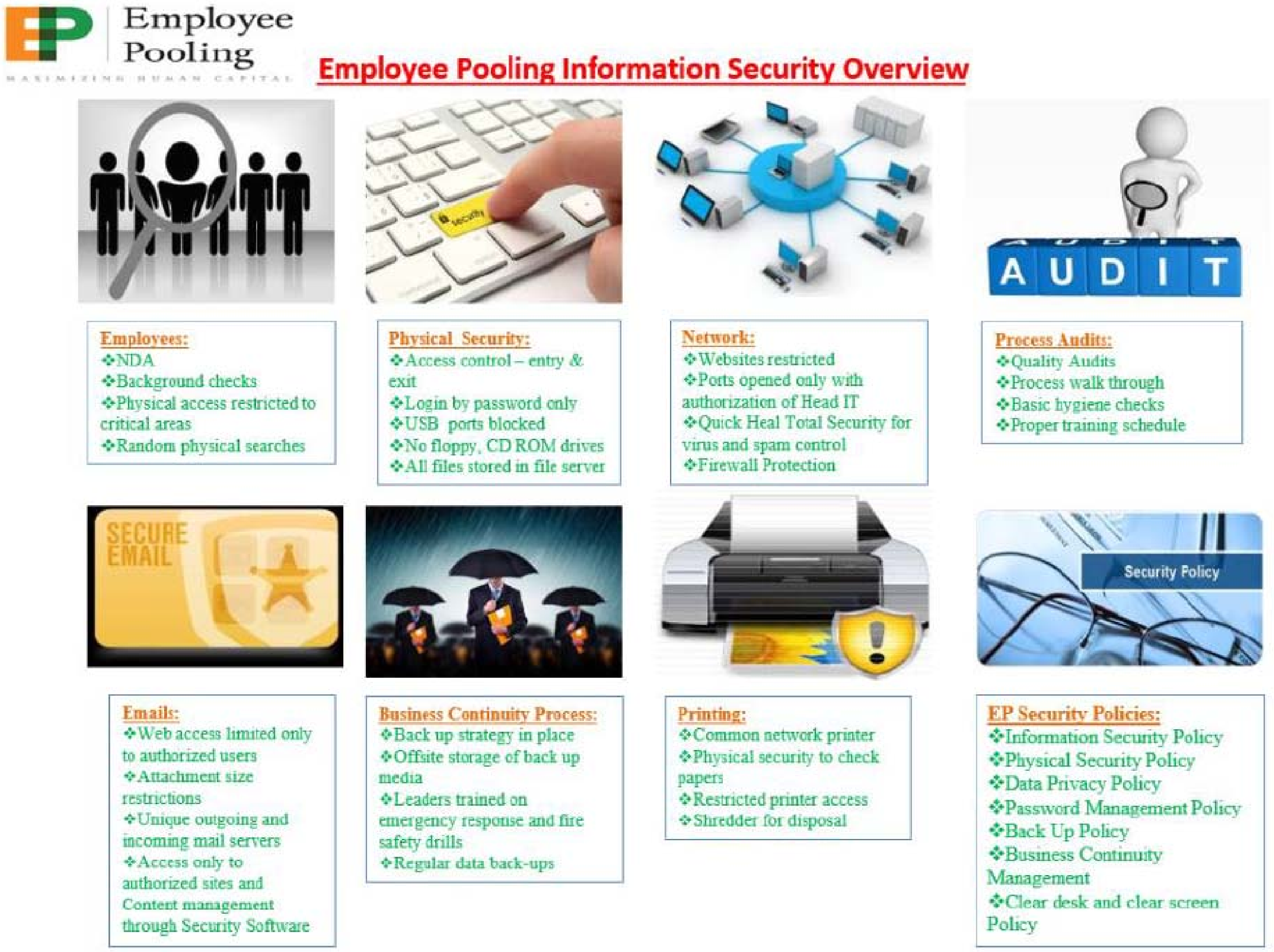
Executive Summary

Employee Pooling, LLC (d/b/a Employee Pooling, “EP”, “EP Insurance Services”, and “EP Mortgage Services”) has been organized and doing business since February 2011 delivering round-the-clock process management solutions for the financial services and mortgage industries. EP delivers its services through its process management center, Employee Pooling Resources Pvt. Ltd. (“EPR”), located in New Delhi, India. The policies in this guide apply only to EPR unless otherwise stated.

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. As such, EP makes administrative, physical, and technical safeguards a priority in all its business dealings to protect client information.

EP provides this security package as a general reference for its prospective customers and current customers 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.

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

1) INFORMATION SECURITY POLICY

POLICY SECTIONS

1.0 APPLICABILITY & IMPLEMENTATION

This policy is applicable for all employees/trainees with Employee Pooling Resources (EPR"). The purpose is to guide the employees in best possible use of IT systems, with less vulnerability, in their routine business operations. The Policy clearly defines which User Group/user, is allowed or restricted access, to a particular IT resource like Internet, Application Software, Databases, Network Administration, e-Mail, Intranet, Information classified on the basis of Confidentiality, Integrity and Availability, as applicable to EPR, on a Need-to-know and Need-to do basis.

1.1 SCOPE

Information Security Management System to support business processes of Insurance services, Application Management services, Case Management services and IT Services. To support all internal processes and operations of EPR being carried out at:

B – 54 New Krishna Park, Vikaspuri,
New Delhi, India – 110018

1.2 POLICY STATEMENT

Management of EPR is committed to the maintenance and preservation of Information security that will cater to the confidentiality, integrity and availability of information assets by creating employee awareness and continuous improvement process

Management of EPR is also committed to ensure all relevant individuals understand the key elements of Information Security and why it is needed, and understand their personal security responsibilities.

1.3 DEFINITIONS

Information Security: Information Security is the attribute of protecting information from a wide range of threats and vulnerabilities in order to ensure business continuity, minimize risks to information and business processes and also ensure confidentiality and integrity of information used in the business. Information security attribute also includes architecting a secure information system that can help in creating and sustaining strategic competitive advantages for the business.

Information Resources (IR): All input, processing and output devices of any information processing system and includes all electronic and paper based storage of information. It also includes all active and passive network components and all devices that are connected to any information processing device either physically or logically. It includes any device capable of receiving e-mail, browsing Web sites, or is otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), telecommunication devices attached to any computing device or as a standalone equipment.

Management Representative (MR): A management representative is appointed and given authority by top management to manage, monitor, evaluate and coordinate the information system and is also responsible for its security. This appointment is to enhance effective and efficient operations of a secure information system, to create accountability and provide an organizational position which is formally charged with responsibility for creating and maintaining relevant ISMS. The representative should periodically report to top management on the status of security in information systems and communicate with employees on matters pertaining to the policies and implementation of security procedures and practices.

Information Security Officer (ISO): Responsible to executive management for implementing information security policies, procedures, guidelines and baselines. The ISO is operationally responsible for maintaining the various parameters that determine the efficacy of ISMS. The ISO will also function as the company's primary point of contact for all information security related matters.

Computer Incident Response Team (CIRT): A team that is put in place by top management comprising of IT Team Lead and Head of Data Security is formally charged with the responsibility of creating and implementing a process that will be triggered in response to any computer security incident.

Team Lead - IT Infrastructure: The Team Lead IT Infrastructure is responsible for overall monitoring of IT Infrastructure, Planning for Disaster Recovery / future requirements / new implementations and security of systems.

Change Management Committee: Responsible to executive management for administering and review any change Implementation, cost and reliability. This committee is comprised of CEO, CFO, COO, Vice President - Operations and Team Lead – IT.

Security Incident: Any violation or deviation from information security policy, procedures, processes, baselines and guidelines can either be an incident in the first instance or can escalate into an incident if left unattended or is compounded with another such violation or deviation. Broadly defined, a security incident is any actual or suspected event that has or is likely to have an adverse effect on any component of information security. Some examples of an information security incident could be attempts to gain unauthorized access to **EP's** information infrastructure or data, irrespective of whether the attempt succeeded or failed; any disruption to normal levels of service; unauthorized use of information technology systems for processing or storing data; unauthorized alteration to data; theft of IT equipment's and documentation storing information that is critical; and change to settings or configuration of hardware, firmware, software and network components.

Access Port: A logical or physical identifier that a computer uses to distinguish different terminal input/output data streams.

Expired Password: A password that must be changed by the user before login completed.

Password: A character string used to authenticate an identity. Knowledge of the password that is associated with a user ID is considered proof of authorization to use the capabilities associated with that user ID.

Password System: A part of system that is used to authenticate a user's identity.

User ID: A unique symbol or character string that is used by a system to uniquely identify a user. The security provided by a password system should not rely on secrecy of the user's ID.

Personal Identification: Password systems used to control access to systems that process or handle classified or other sensitive information must assure the capability to uniquely identify each individual user of the system.

Authentication: Password systems used to control access to systems that process or handle classified or other sensitive information must assure unequivocal authentication of the user's claimed identity.

Password Privacy: Password systems must assure, to the extent possible, protection of the password database consistent with protection afforded the classified or other sensitive information processed or handled by the system in which the password systems operate.

POLICY SECTIONS

1.4 INFORMATION SECURITY AWARENESS

An Information Security Awareness Program helps change organizational attitudes to realize the importance of Information Security and the adverse consequences of Information Security failure. This awareness program is applicable to all supporting documents on Policies and Procedures referenced with this document. Further, awareness reminds users of the importance of Information Security and the procedures to be followed.

Policy-specific activities should be performed to promote information security awareness (the extent to which staff understand the importance of Information Security; the level of Information Security required by the organization and their individual Information Security responsibilities; *etc*. – and act accordingly) across the enterprise. Conducting awareness programs is the responsibility of Human Resource team, in support with ISO.

These activities should be:

- Endorsed by top management
- The responsibility of EPR human resources and ISO.
- Supported by a documented set of objectives
- Delivered as part of an on-going Information Security awareness program
- Kept up-to-date with current practices and requirements
- Aimed at reducing the frequency and magnitude of incidents

1.5 PERIODIC REVIEW, RESPONSIBILITY AND APPROACH

The ISO is the Information Security Policy Owner who has been approved by the management responsible for the development, review and evaluation of security policy. Periodic assessment and review of Information Security Policy will be done at EPR once in 6 months. The review of the information security policy should take account of the results of individual management reviews which also includes:

- Assessing opportunities for improvement of the organizational Information security policy
- Approach to managing information security in response to changes to the organization environment, Business circumstances, legal conditions, or technical environment.
- Information Security audit should be done annually.
- Internal audit will be done as per Internal Audit Procedure.

1.6 ENFORCEMENT

All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the ISO/CIRT.

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of EP Information Resources access privileges, civil, and criminal prosecution.

1.7 OPERATIONAL SECURITY

Responsibilities and procedures for the management and operation of all information processing facilities should be established which includes developing appropriate operating procedures. It should be approved by the management.

1.7.1 INFORMATION PROCESSING AND HANDLING

- Information is classified and labeled with the approved management procedure.

- Segregation of duties is implemented to reduce the risk of negligent or deliberate system misuse.
- Different Business processes in the organization are documented in the form of Process maps.
- Instructions for handling errors arise during job execution, including restrictions on use of system utilities should be in place.
- Contact procedure for the event of unexpected operational or technical difficulties should be in place.

1.7.2 CHANGE MANAGEMENT

The process of controlling modifications to hardware, software, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation. A change for the purposes of this Section is:

- any implementation of new functionality
- any modification of existing functionality
- any removal of existing functionality

- All EP information systems must comply with Change management process.
- All EP corporate documents must have version and appropriate approval signatures.
- Administrative rights to change the system time must be removed from users to ensure message integrity. System time must be synchronized with appropriate project specific time by IT support team.
- Operational systems and application software should be subject to strict change management control.

1.7.3 BACK UP

- Backups should be scheduled regularly.
- All data, operating systems, server, utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates).
- Records of what is backed up and where must be maintained.
- Records of software licensing should be backed up.
- The backup media must be precisely labeled and accurate records must be maintained of backups done and to which back-up set they belong.
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Regular tests of restoring data/software from the backup copies should be undertaken.

1.7.4 NETWORK SECURITY

- Protection of information in networks and the protection of the supporting infrastructure are ensured by appropriate logging and monitoring to enable recording of security relevant activities.
- The ability of Network service provider to manage agreed services in a secure way is regularly monitored.
- Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls, intrusion detection systems.

1.7.5 MEDIA HANDLING

- Media is controlled and physically protected to prevent unauthorized disclosure, modifications, removal or destruction of assets, and interruptions to business activities.
- The contents of any reusable media that are to be removed from the organization should be made unrecoverable.
- Authorization procedure and records should be maintained for any media removed.
- All media are to be stored in a safe, secure environment in accordance with manufacture specifications.
- Disposal of any media should be according to the management approved procedure and it should be logged.

1.7.6 MONITORING

EPR has the right to monitor all the activities of employees, including data transfer through mails, deletion, and modification. All the activities of employees will be logged. Management has the right to revoke any privileges if any non-compliance of policy has been identified.

- Systems are monitored and information security events should be recorded.
- Operator logs and fault logging should be used to ensure information system problems are identified.
- System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.
- Log information is protected to ensure integrity.
- If any penetration testing or vulnerability assessment is done, either internally or externally it should be approved by the management, all the procedures related to security should be implemented, it should be planned, documented, reviewed.

1.7.7 SERVICE DELIVERY MANAGEMENT

- Maintaining the appropriate level of information security and service delivery in line with third party service delivery agreement is implemented.
- Service delivery by the third party includes the agreed security arrangements, service definitions, and service management.
- Procedures are in place to ensure the security is maintained through the transition period for all outsourcing arrangements.
- Service performance level is monitored.
- Service reports produced by the third party are reviewed.
- Identified problems are resolved and managed.

1.8 INCIDENT MANAGEMENT

- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.

- All employees of EPR are responsible for notifying the CIRT to initiate the appropriate incident management action.

- The IT executive of IT Infrastructure is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.

- The CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.

- The IT executive of IT Infrastructure is responsible for initiating, completing, and documenting the incident investigation in coordination with other CIRT members.

- The ISO is responsible for coordinating communications with outside organizations and law enforcement.

- In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the Management.

1.9 ACCESS CONTROL

- Each individual has a separate log-on facility. Passwords shall be a combination of alphabetical, numerical and special characters. Password sharing is strictly prohibited.
- Access to resources or files is given based on Project heads approval either by mail or by written consent.

- All laptop hard disk should be encrypted with the management approved software to avoid loss or misuse of confidential data. Username and Password should be used as an authentication mechanism to view decrypted data.
- Only management team can save data classified as confidential in laptop local drive which undergoes periodic back up using approved software or as per Back up procedure.
- USB ports, floppy drives and CD drives, Print access are disabled by default.
- USB access is permitted only at chief executive level and IT.
- Group Policy is also implemented for the entire departments (Printer resource, storage, etc.)
- The EPR workforce (employees/contractors/volunteers) shall receive access cards, badges and display them properly, so they are clearly visible, at the EPR Divisions/Offices to prevent unauthorized physical access.

1.10 COMPLIANCE

- All relevant application legislation for each information system should be identified.

- Intellectual property rights compliance policy should be in place defining the legal use of software and information products.

- The security of information system should be regularly reviewed against security polices and technical platforms.

- Protection of integrity and prevent misuse of audit tools is ensured.

- All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. There is a right to remove any unlicensed software from any computer system.

- Employee Pooling licenses the use of copies of computer software from a variety of outside companies. Employee Pooling does not own the copyright to this software or its related documentation and, except for a single copy for backup purposes or unless expressly authorized by the copyright owner, does not have the right to reproduce it for use on more than one computer.

- With regard to software usage on local area networks, Employee Pooling shall use the software only in accordance with the license agreement. EPR employees are not permitted to install their own copies of any software onto Company machines.

- EPR employees are not permitted to copy software from company's computers and install it on home or any other computers without prior written consent and proper licensing. EPR employees learning of any misuse of software or related documentation within the company shall notify the Manager of Information Technology or other appropriate person.

- Any EPR employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to Employee Pooling or who places or uses unauthorized software on Company premises or equipment may be subject to disciplinary action. Employee Pooling does not condone and specifically forbids the unauthorized duplication of software.

- Users should not illegally copy material protected under copyright law or make that material available to others for copying. Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. Users should not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the company.

- Unless expressly authorized to do so, User is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets, or other confidential information belonging to EP. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal Economic Espionage laws.

2) Physical Security Policy

2.1 Scope

This policy is applicable to all employees/consultants/contractors trainees and others associated with EPR in terms of physically accessing the Information Processing Facilities of EP or any of its constituents.

2.2 Policy Statement

A balanced information security program must include a comprehensive physical security component. A comprehensive physical security component protects and preserves information, physical assets and human assets by reducing exposure to various physical threats that can produce a disruption or denial of service.

2.3 Physical Entry Controls

HR / Administration Department are responsible for providing adequate physical security in the workplace.

Physical access control procedures shall be implemented at all designated points where personnel access needs to be limited.

There shall be designated security personnel at all entrances who shall be responsible for the following activities every time any person enters/exits EPR premises:

- 'In' entry in the register
- 'Out' entry in the register
- Record third party laptop ID when the person carries a laptop beyond the security check point. This shall be checked with the laptop that is being brought out.
- Attendance details if the person entering / exiting is an employee.
- Recording details of gate passes for carrying company assets outside EPR premises and while returning company assets taken out.
- Frisking, subject to prior approval by EPR management, in case of any suspicious event/reporting of any missing asset.

EPR employees / contractors / consultants / trainees shall receive badges and display them so as to be clearly visible, at all EPR locations.

2.3.1 Visitor Control

All EPR locations shall implement visitor control procedures that will include all of the following features:

- Visitor log maintenance.
- Sign-in/sign-out procedures for all visitors with time recorded.
- Badge with ID number with a request to visitors to always display it while at EP premises.
- Visitors escorted at all times by the assigned persons except when they are assigned to a given work location or conference rooms.

2.4 Secured Offices, Rooms and Facilities

- Ensure controlled access to the facilities and computers, where required.
- Store computers in enclosed locations that can be locked when unattended.
- Do not assume that restrictive logical and physical access to the machine is enough security. Require locked cabinets for data storage media as they contain sensitive data outside of the machine.

- Place computer and associated I/O hardware in locked locations as far as possible.
- Make sure your machine has effective power conditioning, such as an Uninterruptible Power Supply (UPS). Make sure that the UPS or surge protector is designed to handle the highest rated amount of power that is needed in the facility.
- Ensure that an electrical line filter is used to protect against voltage spikes.
- Maintain controls over the environment where the computer is installed and used. Ensure that appropriate temperature, humidity and dust control systems are in place. Always maintain temperature and humidity values within the range recommended by the manufacturer.
- Make sure that the computer is not in a room where it will overheat. Make sure that there is sufficient airflow to all parts of the computer to allow circulation of air. Temperature should be generally 50-80 degrees Fahrenheit (10-26 degrees Celsius).
- Install cooling systems with air filters to protect against dust.
- Make sure that there is an adequate automated fire suppression system.
- Make sure staff is trained in the use of all fire suppression systems.
- Install smoke detectors near machines identified as more critical.
- Do not allow food or drink to be consumed near computers.
- Store all on-site backups in a secure location until moved to off-site storage.
- Store backup tapes away from large metal objects to avoid damage from magnetic fields caused by lightning strikes.
- If you have raised floors or dropped ceilings make sure that walls extend to the ceilings and floors so that they cannot just be climbed over.
- Whenever a user is away from his or her access unit during the day, he or she must protect Employee Pooling information assets by locking his/her system.
- At the end of the workday, each user is required to log off from his or her access unit. If a job must be run unattended after work hours, precautions must be taken to protect the access unit from unauthorized use.
- Divisions and offices that provide access units for public use are responsible for ensuring that these access units are logged off when unattended, and at the end of each workday.
- Users must provide access for technical support staff to install upgrades and improvements to each access unit, upon request.
- Telecommunications equipment should be connected to the utility provider by two diverse routes to prevent failure in one connection path removing voice services.
- Voice services should be adequate to meet local legal requirements for emergency communications.
- CCTV Surveillance systems play an important role in monitoring and reporting incidents regarding security of assets and incidents that violate company policies. These closed circuit television systems are in place in both the floors.

3) Data Privacy Policy

3.1 Introduction

Data Privacy Policy refers to the broad guideline of maintaining the confidentiality of classified data, in meeting the contractual terms and conditions of Customers, and in complying the data privacy legislation, at global level.

3.2 Scope

Data Privacy Policy is applicable to all Users, Internal and External, who have access to data (in any form), categorized as per approved Asset Classification of EP.

3.3 Purpose

The purpose is to guide the employees in controlling the use of Data, that has been classified by EPR, as PUBLIC / INTERNAL / CONFIDENTIAL / HIGHLY CONFIDENTIAL Asset classes and thereby maintain Confidentiality, as the ITES industry demands and ISMS requires, as baseline. The given Asset classification should be duly approved by Top Management, before classifying the assets. Data in EPR's possession should be used only for lawful purposes, not to the detriment of customers, who actually own such data.

Risk Assessment of Information Assets, based on Asset Classification, helps in better control and management of Data Privacy. The Policy covers Data Privacy legislation, as applicable to ITES industry, the world over.

3.4 Enforcement

This policy shall be enforced in such a manner that any violation will be dealt with as it were a serious violation of corporate security policy and will be dealt with accordingly.

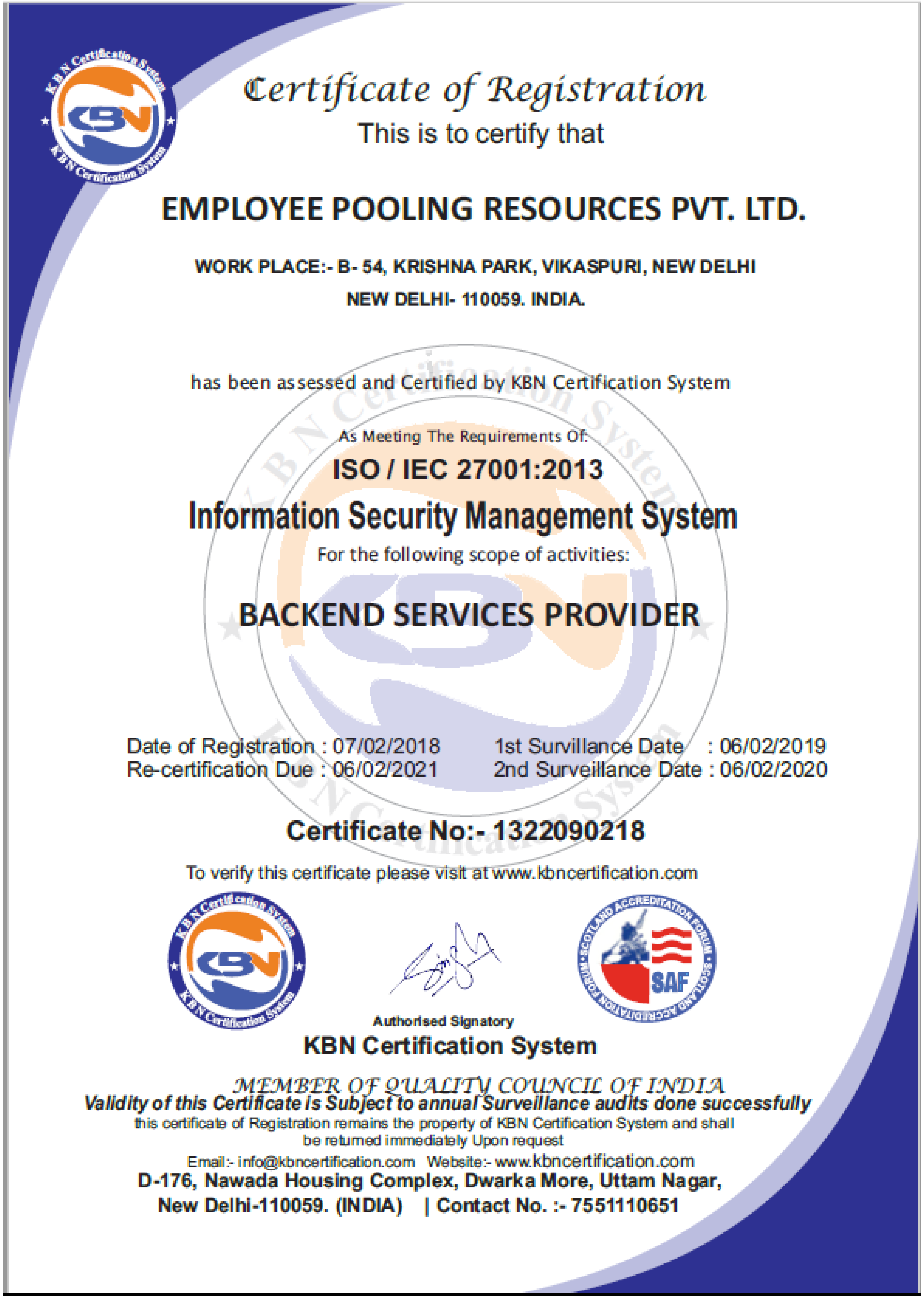
3.5 Revision History

The Management is committed to review this policy and revise it, if needed, on a half yearly basis. Such review and revision will be driven by changing business environment, change in applicable data privacy legislation, or other conditions that are important enough so as not to wait till the next scheduled revision.

4) ISO/IEC 27001:2013 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