PerfectLO.com, LLC.
Information Security Policy

DOCUMENT REF: ITSEC01.7.6
LAST UPDATED: 17-FEB-2018

Executive Owner & Owner
Director of Information Technology
Contact
Director of Information Technology
Revision History

Approval Date	Revision (Name/Section/Description)
14 Feb 2016	
7 May 2016	15.2.1 User Credential
7 May 2016	15.2.2 Logical Security Environment
19 May 2016	15.04.03 Information Technology Services Incident Response
19 May 2016	15.05.05 Server Room Access Policy
19 May 2016	15.06 Portable Computing Device Security
19 May 2016	15.07Acceptable Encryption Policy
19 May 2016	15.03 Risk Assessment and Information Asset Classification
19 May 2016	15.10Technology Equipment Disposal
19 May 2016	15.02.02 Password Use and Protection
10 Jul 2016	15.02.02 Password Expiration
10 Jul 2016	15.14. Clear Desk Policy
9 Jan 2017	15.05.05 Server Room Access Policy -Out of Hours
31 Jan 2017	15.04.04 System and Device Tamper incident response
16 Feb 2017	Yearly review
25 Jan 2018	15.3.4, 1.2 Rewording
17 Feb 2018	Yearly review

Approved by:

17 February 2018	Director of Information Technology

Table of Contents

15.1 Information Security Policy

PerfectLO's information systems, including networks, computer systems and the data they contain, are critical assets that support and advance the business goals of the Company. This Information Systems Security Policy, herein referred to also as the "policy", establishes the principles, control standards and procedures that protect these information systems. The policy document includes the policy definition and the Information Systems Security Standards detailed in sections 15.02-15.13. PerfectLO information systems users, including associates and other parties doing business on behalf of or in support of the Company who have access to these systems, must fully comply with this policy to ensure that the systems and the information they use in the course of their work is protected from unauthorized access, disclosure, modification or destruction.

The Information Technology Manager maintains this policy and its standards. The Information Technology Manager also has the authority to enforce the policy and its associated standards.

15.1.1 Scope

This policy and its associated Information Security Standards apply to all PerfectLO information systems and to all users who have access to those systems.

Violation of this policy will result in disciplinary action commensurate with the severity of the incident, up to and including termination of employment or contracts, in some cases without benefit of a warning, as well as possible criminal or civil penalties.

15.1.2 Statement of Information Security Principles

The following principles articulate the vision underlying the Information Security Policy at PerfectLO. These principles form the basis for all decisions relating to the protection of information systems within the company. All Information Systems Security Standards and procedures are based on these principles.

1. Integrity/Confidentiality/Availability

Information is one of our most valuable assets. Its integrity, confidentiality and availability are essential to our business and to our relationships with associates, company representatives and customers.

The integrity, confidentiality and availability of information are keys to the success of our business. Our ability to get the information we need, when we need it, and in the form, we need it must be guaranteed. Operational procedures and decisions about user access must be balanced by the need for protection and confidentiality and should be guided by the following precepts:

- Need-to-Know: Access will be limited to those users who have a legitimate business need;
- Least Privilege: Users will be given only those privileges required to perform their job function;
- Separation of Duties: Key duties and responsibilities, such as authorizing, processing, recording and reviewing privileged operations or actions, should be assigned to separate individuals.

2. Asset Classification

We have a responsibility to our customers to apply an appropriate level of security to our information assets. All information assets do not require the same level of protection.

Business information asset owners are responsible for both the proper evaluation and categorization of security levels and the application of proper protection to each information asset class. The sensitivity of information assets will be assessed and categorized. Asset classification is a key factor in determining appropriate levels of protection.

3. Risk Assessment

We will determine an appropriate level of protection for our information systems based on a thorough risk assessment.

All information systems will be subject to a standard risk assessment to properly evaluate security risk(s). Risk assessment matrix must be reviewed and maintained to ensure accurate classification of security risk. Information Asset Owners are responsible for understanding the inherent risks both to their assets and to the applications used in the course of their business practice. It is the responsibility of the Information Asset Owner to ensure that a standard risk assessment is completed for all information systems.

The Information Technology Manager is responsible for the review and approval of risk assessments conducted and submitted by Information Asset Owners.

4. Acceptable Use

PerfectLO information systems are intended for authorized business use only. All information stored, transmitted, received, or contained in the company's information systems is the property of PerfectLO and, as such, is subject to company review as required.

Activities that are illegal, unethical, or in violation of any provisions of this policy, are prohibited, including but not limited to the following:

- Accessing, storing or transmitting material that is defamatory, abusive, obscene, profane, sexually-oriented, threatening or racially offensive;
- Collecting and/or transmitting material in violation of any law applicable within the area of jurisdiction;
- Using or reproducing proprietary software or other copyrighted material without the permission of the legal owner or license from the developer;
- Advertising or soliciting for private commercial activities;
- Sending chain letters or forged electronic communications;
- Attempting to test, bypass or compromise system security measures, unless specifically approved in advance and in writing by the Information Technology Manager.

5. Accountability

The responsibility for protecting sensitive information and information processing resources rests on all users of PerfectLO information systems, including PerfectLO employees and other parties doing business on behalf of and in support of the Company. All information systems users will be held accountable for their actions.

All users of PerfectLO information systems must take appropriate care to ensure that the information systems they use in the course of their work are protected from unauthorized access, disclosure, modification or destruction. Careless or deliberate activities that may jeopardize the security of PerfectLO information systems, and/or any failure to comply with PerfectLO Information Systems Security Policy or the PerfectLO IT Acceptable Use Policy will be subject to disciplinary action commensurate with the severity of the incident, up to and including termination of employment or contracts, in some cases without benefit of a warning, as well as possible criminal or civil penalties.

15.1.3 Roles and Responsibilities

The protection of information systems resources is a fundamental responsibility of management, shared by all users of PerfectLO information systems. Specific responsibilities of PerfectLO information systems users are described below.

All users of PerfectLO information systems must:

- Read, understand and comply with this Information Security Policy and its principles, and support its enforcement.
- Comply with all appropriate Information Security Standards and procedures to ensure that PerfectLO information systems and information assets in their business areas are protected from accidents, tampering and unauthorized use or modification. Suspected violations must be reported to the Information Technology Manager.
- Protect the secrecy of personal system passwords by never disclosing or sharing a password with anyone and by changing a password when required by policy or whenever a compromise is suspected.

PerfectLO Management must:

- Identify information assets for which they have primary responsibility.
- Designate Information Asset Owners.
- Ensure that the designated Information Asset Owners and other parties under their supervision are aware of how this Information Security Policy applies to the information systems to which they have access and of their obligation to safeguard PerfectLO information systems.
- Ensure that all individuals under their management authority, including third party contractors and vendors, understand and comply with these policies and standards. Determine and authorize the appropriate level of access required by all individuals under their management authority, including third party contractors and vendors.

Information Asset Owners must:

- Classify and assess information assets in accordance with the Information Asset Classification Standards. The classification of these assets will be periodically reviewed.
- Perform a standard risk assessment for information assets and identify appropriate levels of protection, subject to the review of the Information Technology Manager.
- Implement and manage appropriate business-level controls in order to ensure compliance with the Information Security Policy, and to ensure that sensitive information is disclosed only to those who have a legitimate business need.
- Identify criteria for access to their information assets.

Information Technology Infrastructure and Solutions groups must:

- Implement the security controls necessary to meet the needs of the owners of applications and information assets.
- Provide physical and procedural safeguards for the transfer of information.
- Implement and operate applications and their supporting platform systems in compliance with the Information Security Policy.

15.1.4 Definitions

Availability- The characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner.

Confidentiality- The characteristic of data and information being disclosed only to authorized persons, entities and processes with a right to know at authorized times and in an authorized manner.

Configuration Standard- A documented plan of action for how a standard will be implemented in a given situation. Configuration standards may be developed by division, at the local level or for a specific system, under the direction of the system owner.

Information Asset- Information and data owned by a business unit and stored on a PerfectLO system.

Information Asset Owner- The individual or business unit responsible for the classification, risk assessment and access criteria of an information asset.

Information Systems- The computers, communications facilities, networks, data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for its operation, use and maintenance.

Integrity- The characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

Least Privilege Need to Know- The precept that requires user privileges to be restricted to only those privileges necessary to perform assigned duties. The precept that requires user data access to be limited based on a user's need to access data in the performance of their assigned duties in order to protect the confidentiality of company data.

Policy- A broad statement of principle that presents management's position for each defined control area. Policies are interpreted and supported by standards, guidelines and procedures. Policies are intended to be long-term and guide the development of rules to address specific situations.

Security Event- Any occurrence that requires the attention of Information Security. It may encompass any activity from an individual's system logon to the addition of a server to a network.

Security Incident- A suspected violation of the Information Security Policy.

Separation of Duty- The precept that requires key duties and responsibilities, such as authorizing, processing, recording and reviewing privileged operations or actions, to be assigned to separate individuals.

Standard- A rule that specifies a particular course of action or response to a given situation. Standards are mandatory directives to carry out management's policies and are used to measure compliance with policies.

15.2 User Account Administration

PerfectLO information systems and information assets, including networks, computer systems and the data they contain, must be protected from unauthorized access, modification, disclosure or destruction, to ensure that they are accurate, confidential, and available when required. Access to these systems must be restricted to those who need the information to perform their business functions. The administration of user access to PerfectLO information systems will apply the principles of least privilege, need-to-know and separation of duties.

Access to PerfectLO information systems is controlled by user credentials that are unique to an individual. At a minimum, these credentials consist of a unique User ID and password. All PerfectLO information systems users are required to comply with the standards and procedures for establishing and using their IDs and authenticating their passwords, as described in this document.

15.2.1 User Identification

1. User Credentials: Individual user credentials will consist of a unique User ID and a password. PerfectLO must have records with the user's full name, business relationship to PerfectLO and contact information for all credentials issued to users.
2. Verification of User Identity: Potential user's identities must be verified before new credentials can be issued. The type of verification required will depend upon the sensitivity of the system to be accessed.
3. Composition of User IDs: User IDs will consist of a minimum of three alphanumeric characters, with no maximum other than system-imposed limits.
4. Approval of User ID Request: Management approval is required before new credentials can be issued.
5. System Account Suspension for Failed Login Attempts: User's accounts will be locked after five successive login failures within a period of time specified by the Information Technology Manager. Users will not be able to login until their identity has been verified and their account has been unlocked by an authorized network administrator.
6. External Use of PerfectLO Credentials: User credentials for PerfectLO internal information systems must not be used to access non-PerfectLO information systems.
7. Shared User Credentials: The use of shared user credentials is prohibited. In situations where a shared ID is required, other than for inquiry-only access (e.g., a UNIX root account), the names of the users who have been given the right to the ID, and the reason for doing so, must be documented.
8. Re-use of User Credentials: The re-use of previously assigned user credentials is not permitted.

15.2.2 Password Use and Protection

1. Password Requirement: Passwords are required as a security mechanism to authenticate a user's identity before granting access to PerfectLO information systems.
2. Password Confidentiality: PerfectLO information systems users must protect the secrecy of personal passwords by never disclosing or sharing them with anyone and by changing them when required by policy or whenever there is a suspicion that the secrecy of a password has been compromised. The authorized user is responsible for all actions taken by any party using that authorized user's credentials.
3. Password Composition: PerfectLO information systems users must use the guidelines described in section 15.2.4, as the model for creating their passwords. Passwords must consist of at least eight alpha and numeric characters and must not contain the user's name or user ID. The composition of a new password should be checked at the time it is created, to ensure compliance with this standard. Wherever possible, automatic system validations should be employed to enforce compliance.
4. Password Expiration: Passwords must be set to expire after a maximum of 90 calendar days.
5. Re-use of Passwords: Expired passwords must not be re-used.
6. New and Reset Passwords: New passwords issued by a network administrator must be used for the user's first on-line session. The user must create a new password after authentication and before performing any other tasks. Where possible, system configuration must enforce this requirement.

   User password resets will be performed only by authorized administrators and only when requested by the user to whom the User ID is assigned, after verification of that user's identity. In exceptional circumstances, the user's manager may request a password reset when emergency access is required to a user's account for business-critical purposes. Such managerial requests must be in writing or by attributable and authenticated email from the manager.

   New and reset passwords must be conveyed in a secure manner and must be for one-time use only.

15.2.3 Logical Security Environment

Logical security steps have been defined regarding accessing business system applications. The logical security steps are as follows:

For local network access:
1. A user logs into the network by providing their user ID and password.
2. To access any business system application, the user must log in to the respective application by supplying the appropriate application specific user ID and password

For remote access
1. The user logs into the computer offline
2. When the user is connected to the company network, using Cisco VPN or Secure Remote, they are prompted to enter their user ID, Password and for Secure Remote the security token code as well.
3. Once authenticated, to access any business system application, the user must log in to the respective application by supplying the appropriate application specific user ID and password

15.2.4 Guidelines for Creating Effective Passwords

Password protection is one of the most essential elements in ensuring the security of PerfectLO information systems. As the key to accessing the company's networks, the user password is one of most vulnerable and frequently exploited aspects of any Information Technology Services security program.

If someone learns your password, that person can masquerade as you. He or she can access company information; visit unauthorized web sites; even use your e-mail account to send and receive messages.

This activity presents obvious risks to the company, but there are substantial risks to you, the user, as well.

You will be held responsible for any and all activities that take place under your User ID, regardless of who is using it, including violations of PerfectLO IT Acceptable Use Policy, with which you should already be familiar.

The best way to prevent someone else from using your account is to create an effective password – one that is easy to remember but hard to guess. Use the guidelines below as your model for creating effective passwords.

Note: These techniques are guidelines for creating passwords. You should not use the examples we've provided here as your own password. Use them only as models to create effective, original passwords of your own.

Techniques for Creating Effective Passwords:
1. Use a minimum of eight characters, mixing upper and lower-case letters, numbers (digits), punctuation marks and special keyboard characters. Special keyboard characters consist of the following: *@ # $ % ^ & * _ = + [ ] { } \ | < > /*
2. Use the first letters of the words in a line from a song, a phrase, or a sentence you've made up.
   For example: Seventy-six trombones led the big parade!
   Becomes: S6tltbp!
   Or:
   There are three outs in an inning!
   Becomes: Ta3oiai!
3. Use intentionally misspelled words.
   For example: Two good star actors?
   Becomes: 2gud*Aktirs?

4. Use two or more unrelated words.
   For example: skatesthreeblame
   Becomes: Skates[3]blamE

Things to Avoid in Creating Passwords:

1. Any information that can be easily obtained about you:
   - Your name, family names, names of pets, other proper names or initials
   - Your User ID, user name, group ID or any other system identifier, backward, capitalized, or in any other form
   - Telephone numbers, license or car registration numbers, national insurance number
2. Common or well-known names, identifiers, words or acronyms:
   - Any word that can be found in an English or foreign language dictionary, including slang terms, forward, backward, capitalized or in any other form
   - Months of the year, days of the week or any other aspect of the date, in any form
   - Common acronyms (e.g., LTCP2000, UMASS1989, etc.)
   - Company names, identifiers or references
   - Names of musical groups or sports teams.
3. Any easily guessed sequence of letters, numbers, etc.):
   - More than two consecutive identical characters (e.g., aaadddkkk, etc.)
   - Any word with a number added to it (e.g., 8apples, Lucky7, etc.)
   - Simple keyboard patterns or duplicating characters (e.g., qwerty, ababab, etc.)

15.2.5 Design of Authentication System Interfaces

These guidelines pertain to the management of password systems, including their user interfaces, authentication and storage.

1. Authentication Requirement: Authentication of a user requires that the User ID and password be validated together as a whole. Authentication failure will result in an error message to the user indicating that "Login failed", with no reference to whether the User ID or Password was incorrect.
2. User Password Change: Users of any system or application in which a password is required must be able to change their password after authentication. Users should be prompted to change their passwords before the expiration date. All password changes must be logged where system limitations permit.
3. Password Entry: Passwords must be entered only in non-display fields. The display and printing of passwords must be masked, suppressed or otherwise obscured.
4. Password Storage: Individual passwords must never be stored in a readable form in batch files, automatic login scripts, software macros, terminal function keys, or in computers without access controls. Files containing passwords stored for authentication must be encrypted.
5. Encryption of Transmitted Passwords: Passwords must be encrypted whenever they are transmitted over internal or external networks.

15.2.6 Authorization and Access Controls

1. Requesting Access to PerfectLO Information Systems: Requests to obtain or change access privileges must be authorized by the Information Asset Owner or another appropriate authority. The request must clearly document the access rights required, and a record of all allocated privileges will be kept. Privileges must not be granted until the authorization process is complete.
2. Access Based on a need to know, least privilege and separation of duties: In all cases, the level of access granted will be the minimum appropriate for the business purpose and consistent with PerfectLO Information Security Policy. Privileges will be allocated to individuals based on their need-to-know (i.e., the minimum requirement for their functional role, only when needed), and the scope

of their responsibilities. Access rights will be terminated upon completion of the task or a change in job role.
3. Access Restrictions: Access to PerfectLO production systems and data must be individually determined, based upon criteria defined and documented by the Information Asset Owner, and restricted to authorized users.

15.2.7 Privileged Account Management

1. Privileged Accounts: Privileged Accounts (those with special administrative privileges) are assigned only by Information Technology. Assignment responsibilities must not be delegated.
2. Privileges to be Associated with System Products: Privileged accounts associated with each system product (e.g. operating system, database management system) will be identified, as well as the job roles of users who will be granted the privileges.
3. Special User Identification: User IDs with high privileges should be used only for assignments requiring those privileges. Those privileged users must also be provided with a different User ID for normal business use.

15.2.8 Screen Lock

Screen locks will activate within 10 minutes during user inactivity on all devices.

15.2.9 User Account Status Changes

1. Expired or Inactive User System Accounts: User accounts that have expired or have been inactive for more than 90 days must be disabled to prevent user access. After accounts have been disabled for a period of 30 days, they must be deleted from the system, unless either the user's manager requests that the account be re-activated or there are other operational reasons for the account to be retained. Management authorization is required to re-activate a disabled account.
2. Notification of User Job/Function Changes: User management must follow established notification procedures when a user's job status has changed. User status changes include:
    - Employee transfers
    - Extended absences
    - Terminations (voluntary or hostile separations from the company).
3. Employee Transfers: Credentials of employees and contractors whose responsibilities have been transferred will be modified appropriately upon notification to IT of the transfer of their responsibilities.
4. Extended User Absences: User management must formally notify Information Technology of extended absences (e.g., long-term sick leave, temporary transfers, etc.) to ensure that computer access is temporarily disabled.
5. Termination of User Accounts: All system accounts of permanent and temporary employees and contractors will be disabled when IT are notified of their separation from the company, for any reason.
6. High Risk Terminations: In situations where users with privileged accounts or access to highly sensitive information is terminated, or there is a hostile separation from the company, user management is responsible for directly coordinating with Information Technology to immediately disable the user's account and remove the user's access privileges.

15.3 Risk Assessment and Information Asset Classification

To effectively and consistently protect PerfectLO corporate information assets, a risk management process will be implemented. All business information assets will have a designated owner who is responsible for documenting security risk factors, classifying the asset according to its sensitivity and criticality, and ensuring that appropriate security controls are implemented in order to reduce the risk to an acceptable level.

In determining what security controls are necessary and appropriate for given information assets, the Information Asset Owner must determine the level of residual risk (i.e., the risk that remains after all required security controls have been applied) that is considered acceptable for the business and the corporation. In all cases, however, the security controls that are implemented must comply with the minimum control requirements defined in this document.

15.3.1 Risk Assessment

1. Formal Risk Assessment: A formal (i.e., documented) analysis of PerfectLO information assets will serve as the basis for assessing both security vulnerabilities and the effectiveness of existing and proposed controls. This analysis will result in the identification and prioritization of security needs and a mitigation strategy to reduce the level of risk to an acceptable level.

2. Scope of Risk Assessment: At a minimum, a risk assessment must be conducted for each new application or other new technology introduced into the PerfectLO environment. Risk assessments for existing or legacy systems, applications, and technologies will be performed as considered necessary by the Information Asset Owner or as specifically requested by the IT Manager.

15.3.2 Classification and Protection Policy

Policy: All PerfectLO business information assets must be classified according to its value to ensure that proper protection is afforded during its life cycle.

Minimum Implementation Standards:

Information Classification

1. To ensure that business information assets receive an appropriate level of protection commensurate with the value of the information a determination of classification shall be made for all business information. Business information assets are those that affect and are integral to the following areas:
    - Business growth and competitiveness;
    - Ability to comply with laws and regulations;
    - Integrity and public trust.
2. While not a specific information classification, PUBLIC information is PerfectLO information that is intended for disclosure to the public via open communication sources such as print media or the Internet.
3. All Non-Public information assets shall be classified in accordance with the following criteria and shall be considered PerfectLO “classified” information:

    3.1 CONFIDENTIAL - PerfectLO information which if disclosed to unauthorized parties could cause some harm and thus have a moderate impact on the Company’s interests including competitiveness and business growth, the ability to comply with laws and regulations, and the integrity of and the public trust in the PerfectLO name shall be classified as CONFIDENTIAL.

    3.2 RESTRICTED - PerfectLO information which if disclosed to unauthorized parties could do damage to PerfectLO and thus have a serious impact on the Company’s interests including competitiveness and business growth, the ability to comply with laws and regulations, and the integrity of and the public trust in the PerfectLO name shall be classified as RESTRICTED.

    3.3 HIGHLY RESTRICTED – PerfectLO information which if disclosed to unauthorized parties could do grave damage to PerfectLO and thus have very serious impact on the Company’s interests including competitiveness and business growth, the public trust in the PerfectLO name

and could result in violations that could have legal sanctions shall be classified as HIGHLY RESTRICTED.

4. Classification of Personal Data

   4.1 Policy for the classification of Personal Data is established and entails assignment of Personal Data to one of three Personal Data Types. The types of Personal Data contained in the policy shall map as follows to the classification criteria stated in paragraph [3] above and shall be protected in accordance with the protection requirements for each classification as shown below.

Personal Data Type	Classification
Personal Data Type 1	Information CONFIDENTIAL
Personal Data Type 2	Information RESTRICTED
Personal Data Type 3	Information HIGHLY RESTRICTED

5. Determination of the classification of information assets shall take into account the business needs for sharing or restricting information.
6. Classification Review

   6.1 Information assets shall be evaluated, valued and classified by the Information Owner as necessary to ensure that the proper classification is assigned at all times. It is recommended that a review of the classification of information be performed at least annually.

   6.2 To ensure that appropriate protection is provided, the classification of information shall be determined before use.

15.3.3 Information Owner

1. The Information Owner is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted and otherwise processed.
   1.1. The Information Owner is responsible for determining the appropriate value and classification of the information generated by the owner or Operating Company.
   1.2. The Information Owner shall communicate the information value and classification when the information is released or provided to another entity to help ensure that information protection is provided in accordance with this policy.
   1.3. The Information Owner is responsible for controlling access to his/her information and shall be consulted when other entities wish to extend access authority.
2. The Information Owner shall also consider the potential needs for information integrity, i.e., the potential negative business impacts if business information were deliberately or accidentally modified. The need for access and other controls to ensure information integrity may be significant for all PerfectLO information. Security measures which should be considered for implementation when there is a need for protection against unauthorized modification include, but are not limited to, the following:
   2.1. Approving modification of privilege access, and maintaining a current list of those with such access;
   2.2. Ensuring that an audit trail is automatically logged identifying who made any changes, what changes were made and when they were made.
3. The Information Owner, in assessing the value of an information asset, should also address the potential negative business impacts that may occur if use of the information asset were denied to the Operating Company or its customers and External Business Partners. In some cases, information availability may be a paramount concern, requiring appropriate reliability and security controls no matter the classification.

15.3.4 Information Protection

1. Protective measures shall take into account the business impacts (value) associated with unauthorized access or loss of CONFIDENTIAL, RESTRICTED or HIGHLY RESTRICTED information.

    1.1. Protection of information during transmission: The following requirements apply when CONFIDENTIAL, RESTRICTED, or HIGHLY RESTRICTED information is transmitted electronically.
    1.2. CONFIDENTIAL information may be transmitted electronically over internal network without encryption. Confidential Information sent externally MUST be encrypted.
    1.3. RESTRICTED information shall not be transmitted over a public network (such as the Internet) unless it is encrypted in a manner compliant with the requirements of Acceptable Encryption Policy
    1.4. RESTRICTED information may be transmitted electronically over PerfectLO Network without encryption although it is recommended that Acceptable Encryption Policy-compliant cryptographic protection be used when available.
    1.5. HIGHLY RESTRICTED information shall not be transmitted electronically over any network unless it is encrypted in a manner compliant with the requirements of Acceptable Encryption Policy.
    1.6. HIGHLY RESTRICTED information, transmitted between PerfectLO data centers shall be encrypted in transit in a manner compliant with the requirements of Acceptable Encryption Policy
2. Protection of Information in storage: The following requirements apply when CONFIDENTIAL, RESTRICTED, or HIGHLY RESTRICTED information is stored electronically.
    2.1. CONFIDENTIAL and RESTRICTED information stored within a computer shall be protected either by encryption mechanisms which are compliant with the requirements of Acceptable Encryption Policy

15.3.5 Minimum Security Controls

Minimum security controls will be implemented according to the sensitivity of the asset being protected, as defined in the risk assessment. The minimum control requirements based on asset classification are found in the Control Requirements for Information Asset Classifications Matrix. Where applicable, the controls have been further refined to reflect distinctions within a particular classification level.

15.4 Security Monitoring and Response

To ensure compliance with the Information Security Policy and identify potential vulnerabilities, Information Technology will monitor PerfectLO's information systems activities. This monitoring will detect and prompt the investigation of potential security incidents (suspected violations of the Information Security Policy). Information Technology will then be able to respond appropriately to any security incidents.

15.4.1 Security Event Logging

To effectively monitor systems activities, all security events will be logged to the extent this is possible within system capabilities. Security events encompass everything from an individual's system logon to the addition of a server to a network. All information systems are required to keep security logs of user and system events, so that policy violations can be detected and investigated. These security logs will be used to support the audit process.

1. In the administration and management of logs:
    - Access controls must be in place for all log files.
    - Appropriately authorized administrators must be limited to read-only access to log files.
    - Once created, log files must not be modified.

- Log files should never be overwritten or deleted until they have been archived to off-line storage.
- Security logs must be kept for a minimum of 18 months, or longer as specified by regulatory requirements (e.g., SEC).

2. Event logs must, at a minimum, include:
   - The type of event
   - User ID's for all events
   - Dates and times for events, such as attempts to logon
   - The success or failure of the event
   - Terminal identity or location, if available.
3. At a minimum, the following Security Events have to be logged:
   - All change activity within application systems handling confidential or restricted information
   - All unsuccessful attempts to access confidential or restricted information
   - All successful and unsuccessful attempts to logon to non-public PerfectLO systems
   - All changes to security credentials and their associated attributes, including all password changes
   - All activities performed by special accounts
   - All activities requiring the use of special privileges, including system-initiated events
   - All security administration activity.

15.4.2 Security Monitoring

All PerfectLO information systems must be periodically evaluated by Information Technology to ensure that appropriate security controls are in place.

1. Compliance Monitoring: The Information Technology Manager is responsible for the periodic review of the PerfectLO system security environment for compliance with the Information Security Policy, and procedures. This includes an assessment of:
   - User practices
   - Operations
   - Systems configurations
   - Audits of the administrative process
2. Vulnerability Assessment: Information Technology will conduct a vulnerability assessment of PerfectLO information systems. Periodic checks will be conducted to identify areas of vulnerability and develop a plan to address them. On-going reviews will consist of:
   - Scans and Penetration tests
   - On-going review of and response to published security alerts
3. Incident Detection:
   - Security logs will be monitored to detect and investigate potential security breaches or violations of the Information Security Policy.
   - Intrusion detection systems will be deployed where appropriate to address high-risk vulnerabilities, such as potential attacks from the Internet.
   - All users of PerfectLO information systems are responsible for maintaining a familiarity with the Information Security Policy, and must report any suspected security breaches or violations of the policy.
   - Information Technology will implement a mechanism for communicating apparent security breaches or policy violations. Employees who suspect a security breach or policy violation must immediately communicate their concerns to their manager or another company official as appropriate. The manager will report the incident to Information Technology. In the manager's absence, or in the event of that manager's involvement in the suspected incident, the employee must report the incident directly to Information Technology.

15.4.3 Information Technology Security Incident Response

When suspected security incidents have been detected, Information Technology will implement appropriate procedures to address the problem. The response depends upon the type and severity of the incident.

1. What is an IT security incident?

An IT security incident is any event that leads to, or may lead to, a breach of confidentiality, integrity or availability of information held on an IT system.

Examples of IT security incidents include:

- Theft or loss of IT equipment, software or data;
- Malicious software (e.g. computer virus);
- Willful damage to computer or information held on it;
- Unauthorized use of a computer;
- Unauthorized amendment of information or software held on a computer;
- Unauthorized disclosure of information;
- Deliberate use of another person's password;
- Misuse of software and hardware;
- Playing computer games on PerfectLO computers;
- Use of unauthorized or unlicensed software;
- Non-compliance with policies or guidelines;
- Human errors (e.g. by programmers, system operators or system users);
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Loss of service, equipment or facilities;
- System malfunctions or overloads; and
- Malfunctions of software or hardware.

The response steps to be taken include:

- An IT helpdesk ticket should be created.
- An analysis of all available information to characterize the incident, including its type, scope and source should be included in the ticket
- Communication with all parties that need to be made aware of the incident and its progress
- Collection and protection of information associated with the incident
- Application of short-term solutions to contain the incident
- Elimination of all means of intruder access
- Returning systems to normal operations
- Post-incident analysis and modification of the procedures as appropriate to identify and implement security lessons learned

15.4.4 System and device tamper incident response

If it is suspected that a system or device (Network, storage or other PerfectLO computing device) has been tampered with the following steps should be taken.

- An IT helpdesk ticket should be created.
- The department manager responsible for the equipment should be included on the ticket
- If an alternate system/device can be utilized in place of the suspect system/device this should be employed.
- All passwords allowing access to the system/device should be changed.
- System and event logs should be removed for analysis by the IT department.
- Any and all hardening standards that have been applied to the system/device should be re-affirmed.

- If the system/device contains or processes any customer data the customers who may be affected should be informed, though their account managers.
- Should tampering be confirmed the HR department should be informed.
- Any required HR action will be in line with the relevant HR policies.

15.5 Computing Platforms

Computing Platforms are the architectural base upon which applications are built. Accordingly, the security provided at the platform level is the foundation upon which application security is built. Information Technology is responsible for establishing the security configuration standards for both workstation and server platforms at PerfectLO and for continually monitoring the various platforms to ensure that the appropriate levels of security are maintained.

The Security Standards that follow are intended to protect PerfectLO information systems and assets at the platform level.

15.5.1 Cross-Platform

The security standards that follow apply to both server and workstation platforms.

1. User Authentication: Access to PerfectLO computing platforms must be controlled through the use of an appropriate identification and authentication mechanism (e.g., User ID and Password). Developers must not construct separate mechanisms to collect passwords or User IDs. Nor must they construct or install other mechanisms to identify or authenticate the identity of users without the prior permission of the Information Technology Manager.
2. Standard Configurations: Only PerfectLO supplied hardware and software may be installed on PerfectLO computing platforms.
3. Network Connections: No devices, including server, desktop workstations, laptops, portables, etc., may be connected to any part of the PerfectLO private network without the prior approval of the Information Technology Manager.

15.5.2 Workstations

The following security standards apply to all desktop and portable workstation platforms.

1. Central Administration and Control: Only workstations that are owned by PerfectLO, including desktop and portable computers, may be connected to the PerfectLO private network. These workstations must be centrally administered and controlled by Information Technology. Employees may not switch or trade workstations within or across departments without the approval of the Information Technology Department.
2. Prevention of Unauthorized Use: To prevent the unauthorized use of unattended workstations, employees must log off or lock their workstation whenever they are not physically located at the machine. In addition, all workstations must be configured to use PerfectLO standard, password-enabled screen savers with a ten-minute inactivity time-out.
3. Portable Computers: Employees who use laptop, portable, or other types of computers that can be removed from a PerfectLO facility are responsible for ensuring the protection of PerfectLO information assets stored on these systems. Encryption or other approved computer security utilities should be employed to prevent unauthorized access to sensitive information in the event that the computer is lost or stolen. Similarly, critical business information must be backed up to secure network servers.
4. No Production Applications on Workstations: PerfectLO production software applications must reside on secure servers. Executable functionality for business applications and tools such as the Microsoft Office suite of applications may be executed from desktop workstations and portable

machines, but source software must be protected on multi-user servers that have physical access controls, logical access controls, change controls, and contingency plans.

5. Installing Software Applications: Only Information Technology may install or approve the installation of application software. Other employees must not install software applications of any kind onto a PerfectLO owned workstation, private network directory, or shared network directory. This includes software from a diskette or CD as well as software downloaded from the Internet.
6. Modifying Hardware: Only authorized personnel may install or modify hardware on PerfectLO owned workstations. Other employees may not install or modify the hardware on a PerfectLO workstation; nor may they open a workstation or attempt to service a hardware problem.
7. Anti-Virus Software: PerfectLO standard anti-virus software must be installed and enabled on all workstations. Employees must not attempt to remove, disable, or bypass this software.
8. Configuration Control Software: PerfectLO standard configuration control software must be installed and enabled on all workstations. Employees must not attempt to remove, disable, or bypass this software.

15.5.3 Servers

The following security standards apply to all server platforms.

1. Server Administration: All PerfectLO production servers must be controlled, configured, and centrally administered by the appropriate Information Technology personnel. In addition, non-production servers should be controlled, configured, and centrally administered by the same group.
2. Documented Security Configuration: All servers must be configured in compliance with PerfectLO platform configuration standards. The specific configuration used for each server must be documented and maintained in a secure location.
3. Production Servers: Special consideration must be given to servers used to support production applications. In particular, disks and other on-line storage facilities used on production computer systems should not contain compilers, assemblers, text editors, word processors, or other general purpose utilities which may be used to compromise the security of the system. Similarly, access to systems software utilities must be tightly controlled. Whenever these utilities are executed, the resulting activity must be securely logged and reviewed by the computer operations staff.
4. Destruction of Physical Media: Any physical media (i.e. – Disk Dive), which resides on a server that contains company and/or customer information, that fails will require physical destruction.
    a) Destruction of physical media which contains company information to be verified and signed off by a representative of the PerfectLO Information Technology Department.
    b) Destruction of physical media which contains customer information requires verification and confirmation, as well as sign-off of a representative of applicable company.

15.5.4 Externally Accessible Servers

The following security standards apply to externally accessible server platforms. Externally accessible servers are those that are directly accessible from locations outside the PerfectLO private network. These include but are not limited to Internet servers, remote access servers, and servers that are accessible to PerfectLO business Partners' via a permanent Business to Business connection.

1. Trusted Host Relationships Prohibited: Trusted host and similar services that allow authenticated users on one server to bypass or circumvent the security controls on another server (e.g., shared directory systems that allow a user on one server to access information on another server without authenticating to that server) must not be provided on externally accessible servers without the approval of the Information Technology Manager.
2. Public Servers Must be Placed on Separate Subnets: Publicly accessible servers, such as those that are accessible from the Internet, must be placed on separate, isolated subnets. Firewalls must be used to restrict traffic to and from subnets that contain publicly accessible servers.

3. Disclosure of Information: Information about operating systems, system configuration, software versions, or other internal matters must not be displayed on externally accessible servers until after a user's identity has been successfully authenticated.

15.5.5 Server Room Access Policy

Purpose

The purpose of the Server Room Access Policy is to establish rules and procedures for accessing the Office of Information Technology's server room.

Scope

The Office of Information Technology (OIT) server room is a limited access area. Only personnel requiring constant or regular access to this area have card access to it. All requests for access to the OIT server room area must be approved by the IT Manager.

Policy Statement

Two types of server room access — card and visitor — are permitted. Card access is restricted to OIT staff who require regular access to the server room to perform their job, or WMU emergency personnel for site emergencies only. Visitor access is restricted to non-OIT departmental staff, vendors, or service personnel that are listed on the approved "OIT Server Room Sign-in Access List". Procedures regarding access requests, viewing, or touring the OIT server room are provided below.

Procedures:

Card Access
Individuals with card access to the server room are responsible for ensuring the area remains secure upon entering or exiting. Individuals without server room card access must follow one of the appropriate procedures below.

Visitor Sign-in Access
Individuals on the "OIT Server Room Sign-in Access List" may have monitored access to the server room area. These individuals can enter the server room area with supervision. For each access, they are required to record the following in the server room area log book: date, name, company, reason for entry, in time, and out time. The individual receives a dated visitor badge from the IT staff. The badge must be worn at all times while in the server room, and returned to a member of the IT staff when the individual leaves the server room.

Access Requests
Anyone without card or visitor access must request escorted access prior to being permitted to enter the server room area. If the access request is approved, the visitor must follow the Visitor Sign-in Access procedure and will be escorted at all times by an IT staff member with card access while in the server room.

Viewing or Server Room Tours
Requests for viewing the server room area through the windows must be approved by the IT Manager.

Out of Hours Access

Access to the server rooms outside normal working hours is subject to the preceding procedures. Additionally, access must be approved by either the IT manager or (in the case of departmental server rooms) the head of Department. Visitor access out of hours is permitted provided the above conditions are met and the visitors are accompanied by an authorized member of staff at all times.

Enforcement
Individuals requiring access to the server room, or wishing to view or tour the server room, shall abide by the rules of this policy. Any person found to be in violation of this policy, will be subject to appropriate disciplinary action as defined by current University policy and/or applicable collective bargaining agreements.

15.6 Portable Computing Device Security Policy

15.6.1 Policy

All portable computing devices used to process and store PerfectLO classified information shall be controlled and physically protected and shall be afforded security appropriate to their contents.

Minimum Implementation Standards:

15.6.2 Access

1. Portable computing devices containing PerfectLO classified information shall as a minimum require password authentication in accordance with Password policy before the user is given access to the information.
2. Automatic login scripts, which would allow access to an account without requiring the user to enter his or her password, are prohibited.
3. Portable computing devices shall not be left unattended when remotely connected to the PerfectLO Network even if physically secured.
4. Portable computing devices should be protected in accordance with the value of the information contained in the device.

15.6.3 Protection

1. PerfectLO classified information shall be protected at all times.
2. CONFIDENTIAL and RESTRICTED information stored on removable media (e.g., floppy disks, disks, tapes, flash memory cards, CDs, and USB memory devices) shall either be encrypted using approved encryption in accordance Information Security Policy or the removable media shall be physically protected (e.g., locked in a safe or kept with the individual). HIGHLY RESTRICTED information stored on removable media shall be encrypted using approved encryption in accordance with current policies.
3. Handheld PCs, Palm-size PCs, smartphones, Personal Digital Assistants (PDAs), and other similar devices that can be physically carried by the user shall be protected as one would protect a wallet or similar container that holds one's identity (e.g., driver's license and credit cards).
4. Handheld PCs, Palm-size PCs, smartphones, PDAs, and other similar devices used to store or transmit RESTRICTED or HIGHLY RESTRICTED information (including e-mails and attachments to e-mails) shall comply with all of the Roles and Responsibilities (15.1.3)
5. If the device is synchronized with a personal computer, PerfectLO classified information transferred should be appropriately protected on the personal computer in accordance with the Information Security Policy.
6. Backup of any data stored on a portable computing device is the responsibility of the user and shall be done in accordance with 15.6.3/2.

7. Classified information shall not be accessed on airplanes or in public places, unless the users are certain that only they can read the information on the portable computing device's screen. Do not insert any form of media with unknown identity into corporate equipment.

15.6.4 Reporting Losses

1. Loss of a portable computing device or the loss of removable media that contains classified information shall be reported to the individual's manager and to the IT Manager as soon as possible, but not later than twenty-four (24) hours after detection of the loss.
2. The owner of a computing device or removable media that is reported lost, or whose data are suspected of being compromised, is required to create a helpdesk ticket.
3. In the helpdesk ticket, it should specify the classification of the compromised data, a description of the data, and those parties that might be impacted by the loss (e.g. Finance, Marketing, Public Relations). If Personal Data was stored on the computing device or removable media, HR should be notified. The information in the ticket should also specify whether any mechanisms were in place at the time of the loss or protect the data, such as hard drive or file/folder encryption.
4. If the portable computing device is suspected stolen, a copy of the police report should be provided to the IT department not later than seventy-two (72) hours after the detection of the loss.
5. When good judgment has not been exercised in safeguarding a portable computing device, the individual may be subject to disciplinary action and be held responsible for the replacement cost.

15.7 Acceptable Encryption Policy

15.7.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

15.7.2 Scope

This policy applies to all PerfectLO employees and affiliates.

15.7.3 Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. PerfectLO's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security team.

15.7.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

15.7.5 Definitions

Definition Term: An algorithm that has not been made public and/or has not withstood public scrutiny.

Proprietary Encryption: The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

15.8 Wireless Communication Policy

15.8.1 Overview

The purpose of this policy is to secure and protect the information assets owned by PerfectLO. PerfectLO provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. PerfectLO grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to PerfectLO network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a PerfectLO network.

15.8.2 Scope

All employees, contractors, consultants, temporary and other workers at PerfectLO, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of PerfectLO must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a PerfectLO network or reside on a PerfectLO site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data. The IT must approve exceptions to this policy in advance.

15.8.3 Policy Statement

General Network Access Requirements

All wireless infrastructure devices that reside at a PerfectLO site and connect to a PerfectLO network, or provide access to information classified as 'PerfectLO Confidential', 'PerfectLO Restricted', or 'PerfectLO Highly Restricted':

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use PerfectLO approved authentication protocols and infrastructure.
- Use PerfectLO approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.
- Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to 'PerfectLO Confidential', 'PerfectLO Restricted', or 'PerfectLO Highly Restricted' information must adhere to section 15.3.2.

Lab and isolated wireless devices that do not provide general network connectivity to the PerfectLO network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the DMZ Lab Security Policy or the Internal Lab Security Policy.
- Not interfere with wireless access deployments maintained by other support organizations.

15.8.4 Home Wireless Device Requirements

Wireless infrastructure devices that provide direct access to the PerfectLO corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the PerfectLO corporate network. Access to the PerfectLO corporate network through this device must use standard remote access authentication.

15.8.5 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with PerfectLO.

15.8.6 Definitions

Term Definition

PerfectLO network: A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.

Corporate connectivity: A connection that provides access to a PerfectLO network.

Enterprise Class Remote worker (ECT): An end-to-end hardware VPN solution for remote worker access to the PerfectLO network.

Information assets: Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.

MAC address: The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

15.9 Technology Equipment Disposal Policy

15.9.1 Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of PerfectLO data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

15.9.2 Purpose

This policy has been developed to define the requirements for proper disposal of technology equipment at PerfectLO.

15.9.3 Scope

This policy applies to all technology equipment owned by PerfectLO.

15.9.4 Policy

Technology Equipment Disposal

- When technology assets have reached the end of their useful life they should be sent to the local Information Technology office for proper disposal.
- Information Technology will securely erase all storage mediums in accordance with current industry best practices.
- Equipment which is working, but reached the end of its useful life to PerfectLO, will be made available for purchase by employees.
- A lottery system will be used to determine who has the opportunity to purchase available equipment.
- All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.
- Finance and Information Technology will determine an appropriate cost for each item.
- All purchases are final. No warranty or support will be provided with any equipment sold.
- Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.
- Prior to leaving PerfectLO premises, all equipment must be removed from the Information Technology inventory system.

15.9.5 PerfectLO Ramifications

Failure to properly dispose of technology equipment can have several negative ramifications to the PerfectLO including fines, negative customer perception and costs to notify constituents of data loss or inadvertent disclosure.

15.10 Network Security

PerfectLO private network resources are protected to the highest level of sensitivity required for any information assets connected to or transmitted over them. Since PerfectLO private network is shared by information assets of all classifications, the appropriate level of security is determined by the level of exposure presented by the connection.

The PerfectLO private network includes all network resources owned and /or managed by PerfectLO, including circuits, routers, switches, firewalls, etc.

The level of security implemented for any external connection to the PerfectLO private network is based on an assessment of the sensitivity of the information asset to be communicated and the threat level inherent in the connection. There are three main types of external connection to the PerfectLO private network:

- Public Internet
- Permanent Connections over proprietary networks (e.g., business to business connections, commercial networks, leased data circuits)
- Remote Access (e.g., dialup networks, commercial Internet providers).

15.10.1 Network Configuration and Management

PerfectLO internal network infrastructure is configured to ensure the confidentiality, integrity and availability of the company's information assets. The standards in this section apply to the company's private network and the connection types used to access it.

- Prior Approval Required for All Network Infrastructure Changes: Requests for network infrastructure changes, including installation of analogue or digital lines, must follow the

established change control process with the prior approval of the Information Technology Manager.

- Information Technology Team Review: Information Technology must review and set up all electronic file transfers with businesses or other entities outside PerfectLO private network.
- Control of Physical and Logical Access to Network Equipment: All network resources should be secured from unauthorized access. All PerfectLO internal network devices (routers, firewalls, access control servers, etc.) must have passwords and/or other access control mechanisms established according to the password standards.
- Network Traffic: All communications between PerfectLO private network and external networks must be protected and network traffic restricted by suitable security perimeters and access control mechanisms including, but not limited to, firewalls and router access control lists.
- Publicly Accessible Systems: Publicly accessible servers must be segregated from the rest of the PerfectLO private network.
- Identification of Communication Lines: As a standard documentation requirement, permanent communication lines (e.g., network lines, telephone lines, analogue lines, etc.) must be documented and uniquely identifiable to the PerfectLO system to which they are connected.
- Network Monitoring: Automated tools will be used to monitor the integrity of the network and provide alerts of unusual activity.
- Disable Unnecessary Network Services: Unnecessary network devices or network services must be disabled and/or removed from the private network.

15.10.2 External Connections

The level of security implemented for any external connection to the PerfectLO private network is based on an assessment of the sensitivity of the information asset to be communicated and the threat level inherent in the connection.

- External Access: External access to PerfectLO systems will be provided only through PerfectLO standard gateways, controlled and administered by Information Technology.
- Information Technology Security Approval of External Connections Required: Approval by the Information Technology Manager is required for all direct external connections outside PerfectLO private network, including connections to the Internet or any other external networks.
- External Connections Require Approved Firewalls: All connections between the PerfectLO private network and an external, publicly-accessible network, including the Internet, must be provided through a firewall and/or other approved perimeter security device, as specified by the Information Technology Manager.
- Central Management of Firewalls: All perimeter firewalls must be centrally managed by Information Technology.
- Remote Access: Standard procedures must be followed to acquire and use remote access services to PerfectLO systems.
    - o Authorization is required for any remote access to the PerfectLO private network.
    - o Users must connect only with approved communication equipment and/or software approved by PerfectLO.
    - o Telephone numbers for remote access devices must not be distributed to anyone other than those who have a demonstrated business need to use them.
- Restrictions on Use of Remote Control Software: The use of any personal communications equipment (modems, ISDN cards, etc.) attached directly to personal computers with remote control software will be strictly controlled and in most cases prohibited.

15.10.3 Network Use

- Methods of Accessing the Internet: Methods of accessing the Internet, other than those provided by PerfectLO are prohibited when using PerfectLO computers.

- Dial-in Access: Dial-in access is provided for and may be used for business purposes only. All users must disconnect dial-in connections to PerfectLO when not in use.
- Restriction on Internet Transmission of Non-public Company Information: The transmission of non-public information over the public Internet, including transmission via e-mail, is prohibited unless the information is protected using approved security measures.
- Prohibition on Use of Network Utilities: The installation and/or use of network utilities, including, but not limited to, mapping, scanning and diagnostic tools, to browse or capture information, is prohibited without the prior approval of Information Technology.
- Encryption Products must not be used unless previously approved: Encryption products and processes must not be used to protect PerfectLO information unless first approved by the Information Technology Manager.

15.11 Systems Development

Every application and system developed or purchased for PerfectLO and its affiliates, by either internal or external resources, must comply with PerfectLO Information Security Policy. Security considerations are addressed in each phase of project development or maintenance.

A designated Information Asset Owner must be identified for every project. The Information Asset Owner is responsible for the classification, risk assessment and risk acceptance for the project. Information Technology confirms that the Information Asset Owner has both appropriately assessed the risk to the corporation and fully understands the level of risk being accepted.

Project managers must understand the availability requirements of the new system and the sensitivity of its data in order to design and implement security controls that are appropriate for that system.

The Information Asset Owner who performs the original assessment should review the deliverables for each stage of project development, to ensure that the security assessment results have been addressed as planned and that the risk to the corporation remains unchanged.

When performing application changes, the security impact of any change must be assessed to ensure that the appropriate level of protection is maintained.

15.11.1 Project Planning

Information Asset Owner's Key Tasks: An Information Asset Owner must be identified in the planning stage of all development projects. The Information Asset Owner has the following key tasks to complete.

- Classify the information assets according to documented standards.
- With the help of the project team, identify security needs and potential issues, particularly for those assets classified as restricted or confidential.
- Identify the owners of information assets acquired from other applications. Those asset owners must provide information about the security classification, level of protection and other requirements of the data being shared by their application.
- Ensure that the security classification and level of protection of data acquired from other applications remain consistent with the owning application.

15.12 Third Party Services

All providers of third party products and services for PerfectLO are subject to and must comply with the PerfectLO Information Security Policy. Third parties include:

- Vendor firms providing temporary employees
- Providers of service purchased in conjunction with a product purchase
- Providers of service as part of an on-going support agreement

- Providers of consulting services.

Before any third party can be given access to PerfectLO information systems, all PerfectLO contracts must be finalized and appropriately signed. Third party access will be restricted to only the information and resources required to complete the contracted work, and access will be revoked upon completion of that work.

15.12.1 Selection

- Requirements for Protecting Sensitive Information: As part of PerfectLO selection criteria, third parties requiring access to non-public PerfectLO information must provide information regarding the control structures they have in place for protecting and handling PerfectLO information, including procedures for the return and/or disposition of PerfectLO non-public information. Standard contracts with PerfectLO bind third parties to comply with PerfectLO Information Security Policy.

- Review of Internal Controls: In cases where highly sensitive or critical services or data are being provided by a third party, purchasing may commission or request a review of the service-provider's internal control structure. Information regarding the request and the results of the review must be provided to Information Technology.

- Screening of Third Party Service Providers: As part of the normal third party selection process, the background of unknown third-party service providers must be evaluated. The background information that is reviewed as part of this evaluation should include financial statements, customer referrals, business continuity plans, etc.

- Nondisclosure Agreements: Prior to gaining access to any non-public information, third party service providers must sign confidentiality and nondisclosure agreements that become a term in their contract with PerfectLO.

15.12.2 Contracts

- Awareness of Security Requirements: Contracts with outside service providers will be reviewed to ensure that all Information Security requirements, including access rights, user credentials and potential actions to be taken for security violations, are included in the contract language. All such contracts must allow PerfectLO to terminate the contract for cause if it can be shown that the outside service provider has not complied with these information systems security requirements.

- Security Violations: New contracts with third parties who have previously violated PerfectLO security policies must not be executed without prior authorization by the Information Technology Manager.

- Third Party Notification Responsibilities: Service providers are responsible for immediately informing both the PerfectLO manager responsible for the contract and PerfectLO Information Technology Manager of any information security breaches that have the potential to impact services, systems, or information relating to PerfectLO.

- Employee Reporting of Third Party Violations: Any PerfectLO employee who becomes aware of a third party's security violation must report it.

- Recording Third Party Security Violations: Information Technology will maintain records that outline security problems that have occurred with third parties.

- Release of Systems Documentation to Third Parties: All documentation describing PerfectLO systems or systems procedures is non-public and must not be released to third parties without PerfectLO standard confidentiality and non- disclosure agreements in place.

15.12.3 Access

- Access to PerfectLO Information Systems: Third parties, like all other PerfectLO users, are responsible for the activity performed with their personal User IDs, whether or not these User IDs are connecting via external network facilities. Requests for approval to access PerfectLO private networks and systems must specify the security-related responsibilities of PerfectLO and the third party. Managers must notify Information Technology when third-party access is no longer required.

- Third Party External Connection Privileges: Standard procedures must be followed for third party users to acquire and use remote access privileges to PerfectLO systems. This includes identifying those users as third parties when remote privileges are requested.

15.13 Technology Assessment and Acquisition

The evaluation, selection and acquisition process for PerfectLO information systems and network technologies must include an assessment of security requirements. It is critical that security requirements be clearly specified for all technology products and associated bids or proposals. Vendors under consideration must demonstrate their ability to meet these requirements and to operate in a manner consistent with the PerfectLO Information Security Policy.

15.13.1 Security Requirements:

Hardware and software products must be evaluated on whether they can be installed, configured and operated in compliance with the Information Security Policy. Vendors must not require the modification or abandonment of existing security controls.

15.13.2 Product Support:

Hardware and software components must be obtained from and supported by known and reliable vendors. Vendors must demonstrate that support activities, including installation, maintenance, and procedures for remote and/or onsite access, can be performed in compliance with the Information Security Policy.

15.13.3 Hardware/Software Procurement:

To assure compliance with the Information Security Policy, all hardware and software must be procured through standard purchasing channels.

15.13.4 Vendor Integrity Statements

When third party hardware or software is considered, the vendor must provide written assurances that the product in question does not contain undocumented features and/or hidden mechanisms that could be used to compromise security.

15.13.5 Product Testing

All hardware and software products must be tested before production implementation to ensure that their installation and use presents no adverse impact to the environment

15.14 Security Awareness Training

PerfectLO staff is required to undertake a mandatory annual training on the importance of Information Security. A register will be kept to ensure all staff comply with this requirement. At minimum, the security awareness will include:

- Awareness of security risks and threats
- Identification, prevention and protection actions
- Security best practices and their application
- Data protection (corporate and personal)
- Preservation of confidentiality, integrity and availability
- PerfectLO policies, standards and procedures

Ongoing review of the content will be maintained by the security and compliance team in conjunction with other departments (where applicable) and relevant regulatory, legislative and business requirements.

15.15 Clean Desk Policy

1. Overview
   a) The purpose for this policy is to establish a culture of security and trust for all employees at PerfectLO Limited. An effective clean desk effort involving the participation and support of all PerfectLO Limited employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors. All employees should familiarize themselves with the guidelines of this policy.
2. Purpose
   a) The main reasons for a clean desk policy are:
      i. A clean desk can produce a positive image when our customers visit the company.
      ii. It reduces the threat of a security incident as confidential information will be locked away when unattended.
      iii. Sensitive documents left in the open can be stolen by a malicious entity.
3. Responsibility
   a) All staff, employees and entities working on behalf of PerfectLO Limited are subject to this policy.
4. Scope
   a) At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.
   b) At the end of the working day the employee is expected to tidy their desk and to put away all office papers. PerfectLO Limited provides locking desks and filing cabinets for this purpose.
5. Action
   a) Allocate time in your calendar to clear away your paperwork.
   b) Always clear your workspace before leaving for longer periods of time.
   c) If in doubt - throw it out. Any documentation containing sensitive or confidential information must be placed in the shred bin.
   d) Consider scanning paper items and filing them electronically in your workstation.
   e) Use the recycling bins for sensitive documents when they are no longer needed.
   f) Lock your desk and filing cabinets at the end of the day
   g) Lock away portable computing devices such as laptops or PDA devices
   h) Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
   i) Always collect your printouts from the printer.
6. Enforcement
   a) Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.