[redacted]

[redacted]nd Use Policy

1.0 Password Security Policy

1.1 Overview

Passwords are an important aspect of computer security. They a[redacted]otection for user accounts. A poorly chosen password may result in the comprom[redacted]rporate network. As such, all employees (including contractors and vendors with [redacted] s) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1.2 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system tha[redacted]ess to the [redacted]or stores any non[redacted].

1.3 General Password Construction Guidelines

All passwords must be at least fourteen characters in length, and must contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

All complexity requirements are enforced whenever passwords are changed or created.

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) and user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six months. Each successive password must be unique. Reuse of the same password will not be allowed for ten password changes.

1.4 Password Protection Standards

Do not use the same pa[redacted]or other n[redacted] (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for[redacted] needs. For example, select one password for the E-mail systems and a separate password for network systems. Also, select a separate password to be used for an NT account. You are expected to adhere to the following guidelines:

- NEVER reveal a password over the phone to ANYONE.
- NEVER reveal a password in an e-mail message.
- NEVER talk about a password in front of others.
- NEVER share a password with family members.
- NEVER reveal a password to co-workers while on vacation.
- NEVER write a password in an obvious place that is accessible to others.

All passwords are to be treated as sensitive [redacted]

1.5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action and loss of network privileges.

2.0 Acceptable Use Policy

2.1 Privacy

[redacted]es the right to monitor, duplicate, record and/or log all staff use of [redacted] urces with or without notice. This includes, but is not limited to, e-mail, Internet access, keystrokes, file access, logins, and/or changes to access levels. Staff shall have no expectation of privacy in the use of these technology resources.

2.2 Liability

[redacted] no warranties of any kind, whether expressed or implied, for the services in this policy. In ad[redacted]is not responsible for any damages which staff may suffer or cause arising from or related to their use of [redacted]technology resources. Staff must recognize t[redacted]technology resource usage is a privilege and that the policies implementing said usage are requirements that mandate adherence.

2.3 Staff Responsibilities and Accountability

Effective information security requires full staff compliance. Staff is accountable for any actions and initiated through the use of individual user accounts and/or identification code(s). It is the employee's responsibility to abide by the policies and procedures of all networks and systems with which they communicate. Access of personal or private Internet Service Providers while[redacted] provided information technology resources or using [redacted]provided information technology resources to conduc[redacted]business does not indemnify any entity from the responsibilities, accountability and/or compliance with this or other [redacted]policies. Staff responsibilities include but are not limited to:

- Access and release only the data for which you have authorized privileges and a need to know (including misdirected e-mail).
- Abide by and be aware of all policies and laws (local, state, federal, and international) applicable to computer system use.

[redacted]

- Report information security violations to the Information Security Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of state owned information technology resources.
- Protect assigned user IDs, passwords, and other access keys from unauthorized access.
- Secure and maintain confidential printed information, magnetic media or electronic storage mechanisms in approved storage containers when not in use and dispose of these items in accordance [redacted]olicy.
- Log off of systems (or initiate a password protected screensaver) before leaving a workstation unattended.
- Us[redacted]ed and licensed software.
- Attend periodic information security training provide [redacted] IT Security Branch.
- Follow all applicable procedures and policies.

2.4 Electronic Mail (E-Mail) Policy

T[redacted]ronic mail services (e-mail) policy provides staff with guidelines for permitted use of t[redacted]ology resource. The policy covers e-mail coming from or going t[redacted]nal computers, servers, laptops, paging systems, cellular phones, and any other resource capable of sending or receiving e-mail.

2.5 Ownership

Th[redacted], messages generated on or processed by e-mail systems (including backup copies), and the information they contain. Although staff members receive an [redacted] access the email systems, e-mail and e-mail resources remain the property of the [redacted]

2.6 Monitoring

The [redacted]s, with or without notice, the content of e-mail for problem resolution, [redacted]estigative activities. Consistent with generally accepted business practices th[redacted]collects statistical data about its technology resources. [redacted] [redacted]staff monitors the use of e-mail to ensure the ongoing availability and reliability of the systems.

2.7 Enforcement

Staff may be subject to loss of e-mail privileges and/or disciplinary action if found using e-mail contrary to this policy. Staff must maintain the confidentiality of passwords and, regardless of the circumstances, never share or reveal them to anyone. Larry or a manager must provide express written permission before sensitive information is forwarded to any party outside o[redacted]Staff should contact th[redacted] ith questions regarding the appropriateness of information sent through e-mail.

[redacted]

2.8 Ethical Behavior and Responsible Use

[redacted] c. provides e-mail systems to staff to facilitate business communications and assist in performing daily work activities.

2.8.1 Ethical and Acceptable

- Communications and information exchanges directly relating to the mission, charter, and work tasks of [redacted]
- Announcements of laws, procedures, hearings, policies, services, or activities.
- Notifying staff o[redacted] anctioned employee events, such as the holiday party, bake sales, arts and craft fairs, retirement luncheons, and similar approved activities.
- Respecting the legal protection provided by all applicable copyrights and licenses.
- Practicing good housekeeping by deleting obsolete messages.

2.8.2 Unethical and Unacceptable

- Violating any laws or [redacted]icies or regulations (e.g. those prohibiting sexual harassment, incompatible activities, or discrimination).
- Submit, publish, display, or transmit any information or data that contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material.
- Compromising the privacy of staff, customers, or data and/or using personal information maintained by t[redacted] or private interest or advantage.
- Engaging in any activities for personal gain, performing personal business transactions, or other personal matters (e.g. sending sports pool or other gambling messages, jokes, poems, limericks, or chain letters).
- Intentionally propagating, developing, or executing malicious software in any form (e.g. viruses, worms, trojans, etc.).
- Viewing, intercepting, disclosing, or assisting in viewing, intercepting, or disclosing e-mail not addressed to you.
- Distributing unsolicited advertising.
- Accessing [redacted]nc. e-mail systems (e.g. Hotmail, Yahoo!) [redacted] owned resources.

3.0 Email & Phone Security Policies

3.1 Password Verification

[redacted]rd based on an inbound call alone. If a caller requests a password over the phone, you must adhere to the following protocol to ensure that you are able to verify the identity of the caller:

- NEVER send a requested password via email in response to a request received by phone.
- Phone the caller back at the work number tha[redacted]o verify that they are sitting at their desk). Once you are able to positively identify the caller, you may send them an email to reset their password.

[redacted]

- Contact an administrator at the institution, and request that they give the caller their login information or reset their password. Another party within the institution will be able to confirm that the request is legitimate.

[redacted]

4.0 Physical Security Policy

4.1 Purpose

The purpose of the Physical Security Policy is to provide guidance for Visitors and Employ[redacted] [redacted]premises, as well as for employees sponsoring Visito[redacted]

4.2 Cancellation or Expiration

The processes and statements in this document do not have an expiry date. However, this document is reviewed and updated annually, and is maintained by [redacted]

4.3 Scope

This policy applies to all Visitors and Employees to any premise o[redacted] and to employees who sponsor Visitors.

4.4 Policy Statement

4.4.1 Visitor Check-In

- All Visitors must arrive at the front door. All Visitors must identify, and if requested, provide proof of identity.
- All Visitors must be met by their employee sponsor at the time of Check-In.
- A Visitor cannot sponsor another Visitor.

4.4.2 Photographs and Cameras

Visitors and Employees are not permitted to take photographs insi[redacted] remises, unless discussed specifically with sponsoring employees. For instance, photographs are sometimes required for documentation purposes. If employees have any questions about the suitability of photographs, they should consult Management.

[redacted]

Dedicated cameras are not permitted onsite. Cell phones and laptops equipped with cameras are permitted, but as previously stated; photographs are prohibited except where explicit permission has been obtained.

4.4.3 Information Disclosure

Visitors and Employees should not request information that does not pertain to their visit or the work being performed. Requests of a confidential or otherwise inappropriate nature, including but not limited to corporate documents, customer information, financial projections, comments on any matter currently under litigation, future products or future corporate direction, or information or statements in the name of the company (as might be requested by a reporter or a lawyer) will be reported to the President or Management, and will be dealt with under the "Penalties" section of this document.

4.4.4 Visitor Check-Out

Visitors will check out at the same station where they arrived.

4.4.5 Multiple Day Visits and Longer Term Contracts

Visitors who are [redacted]or multiple days must follow all procedures associated with this policy (Check-In, [redacted]ach day of their visit.

4.4.6 Visitors and Groups Requesting Tours of the Facility

All requests by groups for tours o[redacted]es facility will be referred to Management. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative.

In these cases, a verbal summary of the Emergency Evacuation Procedure and the restrictions on [redacted]mmunicated to the Visitor Group prior to entry of the facility by a pre-designated [redacted]loyee. Any hazard specific to the areas being visited will also be communicated at that time. Visits to areas of this type may require waivers to be signed individually before entry to the facility.

All Visitors or Groups on a tour will be accompanied by their sponsor(s) at all times.

4.4.7 Network or System Access

Consultants or other Visitors that require internet network access: There is no wireless access.

Visitors who require access to production IT networks will need permission from their employee sponsor. Part of this procedure will require the Visitor to review the Acceptable Use Policy. After credentials are arranged, activities on the network will be subject to the Acceptable Use Policy. Visitor use of employee credentials is not permitted under any circumstances.

Visitors who require access to the network will require prior permission from Management. Visitor use of employee credentials is not permitted under any circumstances.

Remote Acces[redacted]tworks are governe[redacted]cess Policy.

4.4.8 On Courtesy

[redacted]

All em[redacted]are to bear in mind at all times that all Visitors are either Customers or potential Customers. Even in the case of clear violations of this policy, all actions, dealings and conversations are to be courteous in nature.

4.5 Responsibility

Employees accept all responsibility for maintaining compliance with the above policy.

4.5.1 Last employee leaving the building.

The last employee to vacate the premises must:

- Turn off all lights
- Secure the door to the break room
- Secure all windows
- Secure the inner front door
- Arm the alarm system
- Secure the front outer door

6.0 Penalties

Violation of any of the requirements in this policy by any employee will result in suitable disciplinary action, up to and including prosecution and / or termination.

Violation of any of the requirements in this policy by any Visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

[redacted]

[redacted]

Security and Use Policy Acknowledgment

Purpose: This document must be signed by all empl[redacted]ogies, Inc. indicating you understand and abide by our security protocol.

This is to be read and signed after reviewing the Security and Use Policy document, as well as security training materials particular to your department. These materials can be found here:

[redacted]

By signing the following I understand and commit to following all of the security procedures listed below:

- Policies and Procedures listed in the Security and Use Policy document.
- FERPA Guidelines.
- No passwords for any of our systems may be stored in written form.
- The front door must remain secured at all times, with access permitted only through use of biometric lock.
- The alarm must be armed before leaving if you are the last person out at the end of the day.
- No personal laptops or external drives (zips/flash/USB/etc.) a[redacted] premises.

Failure to comply will result in disciplinary action up to and including termination.

I have read and understand this communication:

_____ _____

Signature **Date**

_____

Printed Name