

APPENDIX E TO DIR CONTRACT NO. DIR-TSO-2603
ENVIRONMENTAL INTELLIGENCE CLOUD SERVICES AGREEMENT - PART II

TERMS AND CONDITIONS

There are two parts to the Environmental Intelligence Cloud Services Agreement. Part I consists of the Appendix D, Statement of Work and Part II Consists of these Terms and Conditions. These Terms and Conditions are incorporated by reference into the Environmental Intelligence Cloud Services Agreement.

1. Background and Certain Definitions

1.1 Environmental Intelligence, LLC. ("we" or "us") has developed an online system (the "System") for providing Infrastructure as a Service and Cloud Broker Services to DIR Customers. For the purposes of this Terms & Conditions Agreement, "User" is defined as an individual person, to whom credentials and authorized access to EI systems and resources have been provided.

Changes to designated Users or and any other selections, must be communicated and agreed upon in writing. However, if there are increases to the number of Users, select additional Systems or select additional Services, our pricing will increase accordingly. Pricing will be adjusted in accordance with Appendix C, Pricing Index, of DIR Contract No. DIR-TSO-2603, or as agreed upon by the parties.

2. Supplier Licenses

2.1 All Microsoft Applications are subject to the terms of its "Customer License Terms," a copy of which is attached hereto as Exhibit "A." –Use of our Microsoft Licenses are limited to the Microsoft Operating System and Microsoft SQL Service, do not include additional Microsoft Software. Customers may provide their Microsoft software licenses for deployment on our system.

3. Services

3.1 During the Term, we will provide email and/or telephone support, as provided in the Statement of Work, for your Users (all of whom must be individuals) who are listed on Schedule "A," as may be amended, and are thereby authorized to use the Services that you select. Our Customers do not receive direct support from Microsoft or, unless otherwise set forth herein, any other supplier. Customers are allowed to obtain direct support from Microsoft or other supplier for all customer-provided software.

3.2 The number of Users will be the number set forth on Schedule "A" which may be amended, from time to time, by mutual agreement. Each will be required to have a "Key" to use the Service, with their respective Keys, names, titles, office locations and positions provided to us. Each "Key" may be used on only one client computer which is usable by only one person at a time. You are responsible for assuring that Keys we provide to you are used only in accordance with the terms of DIR Contract No. DIR-TSO-2603 and this Agreement.

4. Ownership of Data

4.1 It is understood and agreed that you will own all data produced by your Users use of the Service.

5. Proprietary Rights

5.1 You acknowledge and agree that we, and our suppliers, own all proprietary rights in and relating to the Systems and the Services and in all changes made thereto now or in the future, including, but not limited to, any and all patent, copyright and trade secret rights and in all trade names and marks associated with the Systems and the Services, unless otherwise agreed upon, in writing, by the Parties. In the event that EI develops any custom code for a customer in order to satisfy the customer requirements under the SOW and such custom code resides on EI's system, EI grants the customer full rights to use, modify, and transfer of such customization both during the term of this agreement and perpetually afterward.

5.2 We acknowledge and agree that, subject to your Agreement with your Users, you will own all proprietary rights in all files and data that are produced by your Users using the Systems.

6. Restrictions

6.1 It is understood and agreed that the right to use the Service does not authorize you to, and you agree not to:

(a) Reverse engineer, decompile or disassemble the Systems or permit any other person to reverse engineer, decompile or disassemble the Systems. In this regard, you agree to exert best efforts to prevent anyone from taking that action with respect to any copy of the Systems in your possession, custody or control or through any ability you may have to gain access.

(b) Permit anyone, other than your Users, acting in the course of their employment or otherwise on your behalf, to use any of the Services.

(c) Permit anyone to use the Services to help design a similar service whether for your use, for a competing third-party service or otherwise.

(d) Permit employees and other individuals who are not Users, to use any of the Services.

6.2 You further agree to follow our standard policies and procedures that may be changed from time to time provided they are and remain commercially reasonable. Any changes will require DIR authorization prior to implementation. If the parties cannot reach agreement on any changes, DIR may terminate the Contract.

7. Limited Warranties

7.1 We represent and warrant that we will provide the Services during the Term. SLA's will be established according to the customer requirements and defined in the Statement of Work.

7.2 We have no responsibility for problems with your equipment not provided by us or internet connectivity not provided by us.

8. Limitation of Damages and Other Remedies

8.1 Limitation of Liability will be handled in accordance to Appendix A, Section 8K of DIR Contract No. DIR-TSO-2603.

9. Term and Termination

9.1 The initial "Term" of this Agreement will be for twelve (12) months with three (3) annual renewal options exercised by the Licensor's issuance of thirty (30) days advanced written notice and Customer's concurrence prior to the then-effective expiration date. Any "Trial Period" set forth on Schedule "C" will not be counted as part of the Term and no payments will be required for that period; however, all other terms and conditions of DIR Contract No. DIR-TSO-2603 and this Agreement shall apply to any Trial Period.

9.2 Terminations will be handled in accordance with Appendix A, Section 9B of DIR Contract No. DIR-TSO-2603.

9.4 At any time there is a termination of the Term, you will have thirty (30) days to make copies of all your data, files and other content ("Data") that have been saved by you on one of our servers. You may use the Systems only to save such Data and for no other purpose during such period. After thirty (30) days of termination for any reason, we will have no duty to retain any of your Data on our servers or elsewhere.

10. Reports

10.1 Each month during the Term we will provide you with a report stating what we understand is the number of your Authorized Employees and Independent Contractors. You will either confirm that or point out to us by written notice any discrepancies. In the event of a discrepancy, the parties will work to determine the correct amount owed. In any event you will pay us any amount known to be owed and not the subject of a dispute in accordance with Appendix A, Section 6C of DIR Contract No. DIR-TSO-2603. You will, on a monthly basis, note any changes to the list of Authorized Employees and Independent Contractors.

11. Books, Records and Facilities

11.1 We will be permitted to visit your facility from time to time to verify that you have accounted to us and obtained a license for each of your employees and independent contractors given access to one or more of our Services in any month. In this regard, we will be given access to your records that relate to this issue and may obtain from Customer electronic and documentary copies as we request. Access will be subject to Customer's reasonable requirements including but not limited to issues of security, safety and open records requirements.

11.2 Notices shall be handled in accordance with Appendix A, Section 10 of DIR Contract No. DIR-TSO-2603.

12. Governing Law and Jurisdiction

Choice of Law shall be in accordance with Section 3F of Appendix A, DIR Contract No. DIR-TSO-2603.

13. Force Majeure

13.1 Force Majeure shall be in accordance with Appendix A, Section 9C of DIR Contract No. DIR-TSO-2603.

14. Miscellaneous

14.1 Taxes shall be in accordance with Appendix A, Section 8B of DIR Contract No. DIR-TSO-2603 and Section 4E of DIR-TSO-2603. Assignments will be handled in accordance with Appendix A, Section 3D of DIR Contract No. DIR-TSO-2603. The unenforceability or invalidity of any term, provision, section or subsection of DIR Contract No. DIR-TSO-2603 or this Agreement shall not affect the validity or enforceability of any remaining terms, provisions, sections or subsections, of this Agreement, but such remaining terms, provisions, sections or subsections shall be interpreted and construed in such a manner as to carry out fully the intention of the parties hereto. This Agreement may be executed in counterparts, each of which shall be deemed an original but all of which shall constitute one and the same instrument. The fact of authorship by or at the behest of a party shall not affect the construction or interpretation of this Agreement. No amendments or other change of DIR Contract No. DIR-TSO-2603 or this Agreement shall be effective unless and until set forth in writing and signed on behalf of each of the parties. DIR Contract No. DIR-TSO-2603 and this Agreement embody the entire agreement and understanding of the parties and supersede all prior agreements, representations and understandings between the parties hereto relating to the subject matter hereof.

EXHIBIT "A"

Customer License Terms

TERMS AND CONDITIONS REGARDING USE OF MICROSOFT SOFTWARE

This document governs the use of Microsoft software, which may include associated media, printed materials, and "online" or electronic documentation (individually and collectively, "License Products") provided by Environmental Intelligence, LLC. (hereinafter referred to as "Company") Company does not own the Licensed Products and the use thereof is subject to certain rights and limitations of which Company must inform you. Your right to use the License Products is subject to the terms of your agreement with Company, and to your understanding of, compliance with, and consent to the following terms and conditions, which Company does not have authority to vary, alter or amend.

1) DEFINITIONS.

"Client Software" means software that allows a Device to access or utilize the services or functionality provided by Server Software.

"Device" means each of a computer, workstation, terminal, handheld PC, pager, telephone, personal digital assistance, "smart phone" server or other electronic device.

"Server Software" means software that provides services or functionality on a computer acting as a server.

"Software Documentation" means any end user document included with server software.

"Redistribution Software" means the software described in Paragraph 4 ("Use of Redistribution Software") below.

2) OWNERSHIP OF LICENSED PRODUCTS. The License Products are license to Company from an affiliate of the Microsoft Corporation (collectively "Microsoft"). All title and intellectual property rights in and to the License Products (and the constituent elements thereof, including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporate into the License Products) are owned by Microsoft or its suppliers. The License Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Your possession, access, or use of the License Products does not transfer any ownership of the Licensed Products or any intellectually property rights to you.

3) USE OF CLIENT SOFTWARE. You may use the Client Software installed on your Devices Company online in accordance with the instructions, and only in connection with the services, provided to you by Company. The terms of this document permanently and irrevocably supersede the terms of any Microsoft End User License Agreement that may be presented in electronic form during your use of the Client Software.

4) USE OF REDISTRIBUTION SOFTWARE. In connection with the services provided to you by Company, you may have access to certain "sample," redistribution" and/or software development ("SDK") software code and tools (individually and collectively "Redistribution Software").

YOU MAY NOT USE, MODIFY, COPY, AND/OR DISTRIBUTE ANY REDISTRIBUTION SOFTWARE UNLESS YOU EXPRESSLY AGREE TO AND COMPLY WITH CERTAIN ADDITIONAL TERMS CONTAINED IN THE SERVICES PROVIDER USE RIGHTS ("SPUR") APPLICABLE TO COMPANY, WHICH TERMS MUST BE PROVIDED TO YOU BY COMPANY. Microsoft does not permit you to use and Redistribution Software unless you expressly agree to and comply with such additional terms, as provided to you by Company.

5) COPIES. You may not make any copies of the License Product; provided, however, that you may (a) make one copy of Client Software on your Device as expressly authorized by Company; and (b) you may make copies of certain Redistribution Software in accordance with Paragraph 4 (Use of Redistribution Software). To the extent allowable under record retention laws and policies, you must erase or destroy all such Client Software and/or Redistribution Software upon termination or cancellation of your agreement with Company, upon notice from Company or upon transfer of your Device to another person or entity, whichever occurs first.

6) LIMITATIONS ON REVERSE ENGINEERING, DECOMPIATION AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the License Products, except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.

7) NO RENTAL. You may not rent, lease, lend, pledge, or directly or indirectly transfer or distribute the Licensed Products to any third party.

8) TERMINATION. Terminations will be handled in accordance with Appendix A, Section 9B of DIR Contract No. DIR-TSO-2603.

9) NO WARRANTIES, LIABILITIES OR REMEDIES BY MICROSOFT. ANY WARRANTIES, LIABILITY FOR DAMAGES AND REMEDIES, IF ANY, ARE PROVIDED SOLELY BY COMPANY AND NOT BY MICROSOFT, ITS AFFILIATES OR SUBSIDIARIES.

10) PRODUCT SUPPORT. Any support for the License Products is provided to you by Company and is not provided by Microsoft, its affiliates or subsidiaries.

11) NOT FAULT TOLERANT. THE LICENSED PRODUCTS MAY CONTAIN TECHNOLOGY THAT IS NOT FAULT TOLERANT AND ARE NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE IN ENVIRONMENTS OF APPLICATIONS IN WHICH THE FAILURE OF THE LICENSED PRODUCTS COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL, PROPERTY OR ENVIRONMENTAL DAMAGE.

12) EXPORT RESTRICTIONS. The License Products are of U.S. origin for purposes of U.S. export control laws. You agree to comply with all applicable international and U.S. laws that apply to the License Products, including the U.S. Export Administration Regulations, as well as end-use, end-user and destination restrictions issued by the U.S. and other governments. For additional information, see <http://www.microsoft.com/exporting/>.

EXHIBIT “B”

Acceptable Use Policy for Environmental Intelligence, LLC and all related sites owned, operated or controlled by Environmental Intelligence, LLC

Acceptance of Terms Through Use

This Acceptable Use Policy is used in conjunction with the terms and conditions agreement. Violating any of these policies grants Environmental Intelligence the authority to take action to restrict or terminate your access to Environmental Intelligence services.

Environmental Intelligence, LLC disclaims, to the maximum extent permitted by law, all warranties, representations or other endorsements, express or implied, with regard to the information accessed from, or through, this service, the systems which provide it and the Internet, including all warranties of merchantability or fitness for a particular use. Environmental Intelligence does not assume any liability for the completeness, accuracy or usefulness of any information disclosed or materials accessed. In no event shall Environmental Intelligence (or any persons or entities related thereto) be liable for any special, indirect, or consequential damages associated with or arising from use of this service in any way, including any loss of use, data or profits, regardless of the form of action. Any failure by Environmental Intelligence to enforce this policy in every instance in which it might have application does not amount to a waiver of Environmental Intelligence’s rights.

Lawful Use

You must use this site and Environmental Intelligence Services in accordance with the terms of DIR Contract No. DIR- TSO-2603 and this Appendix E, and in accordance with all federal, state and local laws, ordinances, and regulations.

User Conduct, Prohibited or Unlawful Use

Use of this site and / or Environmental Intelligence Services are for lawful and authorized purposes only, and any other use is strictly prohibited.

Specifically, you may not:

- Attempt to use or gain unauthorized access to data, accounts, hosts, servers, systems or networks of this site, or to probe, scan or test the vulnerability of a system or network of this site, any Environmental Intelligence Services or those of any other party
- Interfere with service to any user, host or network including, without limitation, mail-bombing, flooding, or attempting to overload the system
- Forge any TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting
- Falsify address information or otherwise modify e-mail headers to conceal the sender's or the recipient's identity

Additionally, you may not, by use of any Environmental Intelligence Service or another service, upload, post or otherwise distribute or facilitate distribution of any content, including text, communications, software, images, sounds, data, or other information that:

- Victimizes, harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, gender, sexual orientation, race, ethnicity, age, disability or any other reason
- Contains viruses, corrupted files, or any other similar software or programs that may damage the operation of another's computer
- Violates the terms of the CAN-SPAM Act. Mass distribution of emails for legitimate business purposes are allowed.

EI will not be held responsible for meeting SLA's outlined in customer's SOW to the extent that EI's failure to meet a specific SLA is solely and directly caused by the customer's violation of the terms of use herein.

PLEASE NOTE: The transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender, including those provided by the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM") (P.L. 108-187) or Computer Fraud and Abuse Act (18 U.S.C. § 1030 et seq.); the Virginia Computer Crimes Act (Va. Code Ann. § 18.2-152.2 et seq.) (amended effective July 1, 1999); the Washington Commercial Electronic Mail Act (Wash. Rev. Code Chapter 19.190 et seq.); and any other applicable statutes and regulations.

Environmental Intelligence will notify customer prior to performing any system testing and maintenance pertaining to the distribution of any bulk emails that are suspected as being in violation of the CAN-SPAM Act.

The purpose of such testing includes, but is not limited to, testing of mail servers or proxy servers for unrestricted third party relaying. Environmental Intelligence will ensure that such testing will not adversely affect Service provided to Customer or compromise the security of Customer's network. Customer may be required to correct any system vulnerability upon notification and/or suspend or terminate operations of a known compromised system.

Customer shall have sole control over and bear all liabilities pertaining to Customer Content. Except with Customer's prior written consent, or for normal system administration and customer support purposes, or by court order, Provider shall not access, view, supplement, modify or alter any of the Customer Content that has been provided by Customer to Environmental Intelligence. Nothing in this Agreement will serve as a transfer or assignment of any rights in the Customer Content to Environmental Intelligence.

Unlawful or Unauthorized Use: The Company may discontinue the furnishing of Service, when necessary to take such action to prevent the unlawful or unauthorized use of Service, by blocking traffic to or from certain countries, cities, NXX exchanges, or individual telephones; by blocking call origination; or by blocking calls using certain Customer authorization or access codes. The Company also may suspend the origination of domestic or international traffic associated with any or all Services if necessary to prevent the unlawful or unauthorized use of the Service due to the failure, in whole or in part, of any fraud detection system utilized by the Company to provide or support Service. In the event of any permanent discontinuance, or permanent termination of Service, additional fees will be charged, or refunded in accordance with the terms for Termination in Appendix A, Section 9B of DIR Contract No. DIR- TSO-2603.

International Use

Environmental Intelligence makes no representation that materials available on this site or any or through any Environmental Intelligence service are appropriate or available for use in locations outside the United States, and accessing them from territories where their contents are illegal is prohibited. Those who access this site or any site hosted by Environmental Intelligence from other locations are responsible for compliance with local law.

Intellectual Property Rights

Trademark: Environmental Intelligence; the Environmental Intelligence design logo; and all other related names, design marks, product or feature names are either registered trademarks or trademarks of Environmental Intelligence in the United States and/or other countries.

Environmental Intelligence marks may not be used without the express written permission of Environmental Intelligence. All other products and services referenced in this site are the trademark or services marks of their respective owners.

You acknowledge and agree that copyrights, trademarks, service marks, patents, trade secrets, and other proprietary rights and laws protect all content and materials available on this site or through any Environmental Intelligence service. Nothing on any Environmental Intelligence website shall be interpreted or implied in such a way as conferring any license or right to any intellectual property rights or license to any intellectual property, content, technology, system, process, or related material belonging to Environmental Intelligence by virtue of it being displayed or made accessible on any Environmental Intelligence website. Except as expressly authorized, you agree not to use this site or any Environmental Intelligence services in any manner that would infringe, violate, dilute or misappropriate any such rights, with respect to any material, which you may access, receive or make available through this site or any Environmental Intelligence services.

If you use a domain name or content in connection with the Environmental Intelligence web hosting, or any other web hosting service, you must not use that domain name or content in any way which violates any trademark, service mark, or similar rights of any third party.

Internet Relay Chat Rules

You must not use any programs that may or will interfere with another's use of this site or Environmental Intelligence services. You must not run any Internet Relay Chat ("IRC") robot on any IRC server which might interfere with the Services or otherwise violate this AUP. When logged into any IRC server, you must comply with the rules and policies established by that IRC's service administrator.

Notices

Notices shall be in accordance to Appendix A, Section 10 of DIR Contract No. DIR- TSO-2603.

General Complaints: Please send reports of any activity in violation of this Acceptable Use Policy to Environmental Intelligence's offices or to support@goeillc.com. Environmental Intelligence will reasonably investigate incidents involving such violations. Environmental Intelligence may involve and will cooperate with law enforcement officials if any criminal activity is suspected. Violations may result in criminal and civil liability.

Copyright/Trademark Infringement Complaints: If you believe that your copyright or trademark has been used by an Environmental Intelligence customer without permission, such that the use may constitute infringement of your intellectual property rights, please see the instructions on how to send your claim.

Fraud Complaints: Environmental Intelligence recognizes that acts of fraud can be and are committed over the Internet. Environmental Intelligence encourages all Customers and Internet users to be vigilant about protecting their personal information, account numbers, id's, passwords, etc. As with non-Internet fraud, fraud complaints are best and most appropriately made to law enforcement authorities. If you believe you have been the victim of Internet fraud (either via the web or through email), Environmental Intelligence encourages you to contact your local or state consumer protection authority, or one among several U.S. agencies that handle complaints about Internet fraud, including:

- Federal Trade Commission (FTC) Complaints about consumer fraud (e.g. related to retail, banking and other on line activity) can be filed with the FTC at <https://www.ftccomplaintassistant.gov/#crtn&panel1-1>
- Internet Fraud Complaint Center (IFCC) is a joint effort of the FBI and the National White Collar Crime Center; complaints about Internet fraud may be filed with the IFCC at <https://ic3.gov/default.aspx>
- Securities and Exchange Commission (SEC) complaints related to buying and selling of securities, and related on line activity, can be filed with the SEC Enforcement Division Complaint Center at <http://www.sec.gov/complaint/select.shtml> as well as, your state securities regulators (to locate your state securities regulator, go to <http://www.nasaa.org/about-us/contact-us/contact-your-regulator>

4.0 INDEMNIFICATION

4.1 Indemnification shall be handled in accordance to Appendix A, Section 8A of DIR Contract No. DIR-TSO-2603.

EXHIBIT "C"

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of your company's entire corporate network. As such, you agree to have all employees (including contractors and vendors with access to your systems) be responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Additionally, if you ask us to use any policy that is less secure than what is outlined below, you agree to accept full responsibility for any and all consequences resulting from not adhering to this policy.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 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 that resides at any your facility, has access to the company's network, or stores any non-public company information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 180 days.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "Company Name", "city name" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:~<>?.,./)
- Are at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use these examples as passwords!

B. Password Protection Standards

Do not use the same password for Company accounts as for other non-Company access (e.g., personal ISP account, benefits, etc.). Where possible, don't use the same password for various access needs.

Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every 180 days.

If an account or password is suspected to have been compromised, report the incident to Environmental Intelligence Support and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Environmental Intelligence or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. System and / or Application Development Standards

System and / or Application developers must ensure their programs contain the following security precautions:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

5.0 Enforcement

Failure to follow this policy is in violation of Environmental Intelligence's Terms of Service Agreement and could result in termination of services.

6.0 Definitions

System Administration Account - Any account that is for the administration of a System (e.g., Oracle database administrator, ISSU administrator).