SECURITY POLICY

INTRODUCTION

This Allied Colo LLC Security Policy (the "Policy") defines acceptable practices relating to the location by the customers (the "Customers" or "you") of Allied Colo LLC and all of its affiliates (including, but not limited to, direct or indirect subsidiaries and parents), owners, managers, members, directors, officers, employees and professional advisers ("Allied Colo," "we" or "our") of their equipment (the "Customer Equipment") at locations leased or owned by Allied Colo (the "Customer Locations" or "Locations") and the use by such Customers of the services provided by Allied Colo to its Customers at such Locations (the "Service") and by users that have gained access to the Service through Customer accounts (the "Customer's Users" or "Users"). By locating its Customer Equipment in the assigned Customer Location and by using the Service, you acknowledge that you and your Users are responsible for compliance with the Policy and that you have indemnified Allied Colo against any claims arising from any violation of this Policy as specified in the Allied Colo Master Services Agreement executed by all Customers prior to the location of their respective Customer Equipment in the applicable Customer Location (the "Master Services Agreement"). Undefined capitalized terms used herein shall have the meanings respectively given to them in the Master Services Agreement.

Comment [ST1]: Legal needs to re-write this so that it addresses specifically the SECURITY posture outlined in this document.

PORTAL ACCESS RECOMMENDATIONS

Minimum Password Length

The length of passwords should always be checked automatically at the time that users construct or select them. All passwords should have at least eight (8) characters.

Passwords Should Change Periodically

As a security precaution, Customer-chosen passwords should be changed at least every 90 days.

Difficult-To-Guess Passwords Recommended

All Customer-chosen passwords for computers and networks should be unique and difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456" should not be employed. Likewise, personal details such as spouse's names, automobile license plates, social security numbers, and birthdays must not be used unless accompanied by additional unrelated characters. Customer-chosen passwords should also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang should not be employed.

Cyclical Passwords Discouraged

Customers are discouraged from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change. In these prohibited passwords, characters which change are typically based on the month, a department, a project, or some other easily-guessed factor. For example, users should not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.

Customer-Chosen Passwords Should Not Be Reused

Customers should not construct passwords that are identical or substantially similar to passwords that they had previously employed.

Passwords Never In Readable Form When Outside Workstations

Fixed passwords should never be in readable form outside a personal computer or workstation (e.g. sticky notes).

Prevention Of Password Retrieval

Computer and communication systems should be designed, tested, and controlled so as to prevent both the retrieval of, and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

Password Sharing

Regardless of the circumstances, passwords should never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If a password is provided to a Allied Colo IT support representative in order to help diagnose a specific user issue, that user should change their password immediately after the issue is resolved.

Customers Responsible For All Activities Involving Personal Customer-IDs

Customers are responsible for all activity performed with their personal Customer-IDs. Customer-IDs may not be utilized by anyone but the individuals to whom they have been issued. Customers should not allow others to perform any activity with their Customer-IDs. Similarly, Customers are forbidden from performing any activity with IDs belonging to other Customers.

Removal of User-ID for Termination or Job Change

Customers must notify Allied Colo immediately upon termination or a job change of one of its personnel such that they will no **longer require system's access**. Upon receipt of notification, Allied Colo will immediately deactivate and remove the Customer- ID from the system.

Allied Colo Password Management

All Allied Colo controlled passwords (e.g. server root passwords, network device passwords, client access passwords) will be stored encrypted and not be produced in printed format. Passwords will never be shared between Allied Colo employees and/or Customers in clear text format. PGP is the general standard Allied Colo uses to encrypt data and pass data securely between both employees and clients.

PRIVILEGE CONTROL

Third Party Access To Allied Colo Systems

Before any third party is given access to Allied Colo computer systems, written agreement to abide by Allied Colo' Rules and Regulations must have been signed by a manager at the third-party organization.

Support For Special Privileged Type Of Users

All multi-user computer and network systems must support a special type of user-ID which has broadly-defined system privileges. This user-ID will in turn enable authorized individuals to change the security state of systems. The number of privileged user-IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

Restriction Of Special System Privileges

Special system privileges, such as the ability to examine the files of other users, must be restricted to those directly responsible for system management and/or security. File access control permissions for all Allied Colo computer

systems must be set to a default setting which blocks access by unauthorized users. Beyond that which they need to perform their jobs, computer operations, hardware and systems support staff must not be given access to--nor permitted to modify--production data, production programs, or the operating system.

Unbecoming Conduct And The Revocation Of Access Privileges

Allied Colo reserves the right to revoke the privileges of any user at any time. Conduct that interferes with the normal and proper operation of Allied Colo' information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others are among types of conduct that will not be permitted.

Termination Of User Processes Or Sessions And Removal Of User Files

Allied Colo systems administration staff may alter the priority of, or terminate the execution of, any user process which it reasonably believes is consuming excessive system resources, significantly degrading system response time, or if this usage is deemed to be in violation of security policies.

Maintenance Of Master User-ID And Privilege Database

So that their privileges may be expediently revoked on short notice, records reflecting all the computer systems on which users have user-IDs must be kept up-to-date.

INTELLECTUAL PROPERTY RIGHTS

Information As An Important Allied Colo Asset

Accurate, timely, relevant, and properly protected information is absolutely essential to Allied Colo and its Customers. To ensure that information is properly handled, all accesses to, uses of, and processing of Allied Colo internal or Customer information must be consistent with Allied Colo information systems related policies and standards.

DATA PRIVACY AND CONFIDENTIALITY

Notification Of Suspected Loss Or Disclosure Of Sensitive Information

If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the owner of such information and [Allied Colo Management] should be notified immediately.

DATA INTEGRITY

Right To Remove (Offensive) Material Without Warning

Allied Colo Management retains the right to remove from its information systems any material it views as (offensive) or potentially illegal. Examples of such potentially illegal activity is outlined in the Allied Colo Acceptable Use Policy.

No Responsibility For Monitoring Content Of Information Systems

Allied Colo Management reserves the right to remove any message, file, database, graphic, or other material from its information systems. At the same time, Allied Colo Management has no obligation to monitor the information content resident on or flowing through its information systems.

Security Requirements For Network-Connected Third Party Systems

As a condition of gaining access to the Allied Colo computer network, every third party must secure its own connected systems in a manner consistent with Allied Colo requirements. Allied Colo reserves the right to audit the security measures in effect on these connected systems. Allied Colo also reserves the right to immediately terminate network connections with any third-party systems not meeting such requirements.

Standards Of Common Carriers Do Not Apply

The networking services provided by Allied Colo are provided on a contractual carrier basis, not those of a common carrier. As the operator of a private network, Allied Colo has a right to make policies regarding the use of its network systems without being held to the standards of common carriers.

Standard Encryption Algorithm & Implementation

If encryption is used, government-approved standard algorithms (such as the Data Encryption Standard or DES) and standard implementations (such as cipher-block chaining) must be employed.

Disclosure Of Encryption Keys Requires Special Approval

Encryption keys are a most sensitive type of information, and access to such keys must be strictly limited to those who have a need-to-know. Unless the approval of Allied Colo is obtained, encryption keys shall not be revealed to consultants, contractors, or other third parties.

Time Period For Protection Of Encryption Keys Used For Confidentiality

The secrecy of any encryption key used for confidentiality purposes (e.g., for data encryption or as a seed to an access control system) must be maintained until all of the protected information is no longer considered confidential. Users must not allow automatic backup systems to make a copy of the readable version of their private key used for digital signatures and digital certificates. Automatic backups could allow unauthorized transactions to be generated in the involved users' names. These backups are prevented by keeping private keys in smart cards or otherwise in encrypted form.

Prevention Of Unauthorized Disclosure Of Encryption Keys

Encryption keys must be prevented from unauthorized disclosure via technical controls such as encryption under a separate key and use of tamper-resistant hardware.

Explicit Assignment Of Encryption Key Management Functions

Whenever encryption is used to protect sensitive data, the relevant owner(s) of the data must explicitly assign responsibility for encryption key management.

Digital Certificate For All Allied Colo Internet Web And Commerce Sites

A current digital certificate is recommended for both Allied Colo and client Internet servers handling confidential information.

Required Reporting of Information Security Incidents

All suspected Information Security incidents must be reported immediately to Allied Colo Management.

Centralized Reporting Of Information Security Problems

Information Security is the inability of unauthorized third parties to access any documents, data or other information stored or otherwise normally available to authorized parties on Allied Colo network or any Allied Colo infrastructure components. All known vulnerabilities - in addition to all suspected or known violations - must be communicated in an expeditious and confidential manner to Allied Colo Management. Unauthorized disclosures of Allied Colo information must additionally be reported to the involved information owners. Reporting security violations, problems, or vulnerabilities to any party outside Allied Colo (except external auditors) without the prior written approval of the Allied Colo Legal Department is strictly prohibited. No external reporting of any Information Security violation or problem may occur without written consent of Allied Colo Management.

Required Investigation Following Computer Crimes

Whenever evidence reasonably shows that Allied Colo has been harmed by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that Allied Colo Management can take steps to ensure that: (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Information Ownership And Management's Responsibilities

All production information possessed by or used by a particular client must have a designated owner. Owners must determine appropriate sensitivity classifications as well as criticality ratings. Owners must also make decisions about who will be permitted to access the information, and the uses to which this information will be put. Owners must additionally take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information. Designated owner lists are to be provided to Allied Colo Management and reviewed on at least an annual basis.