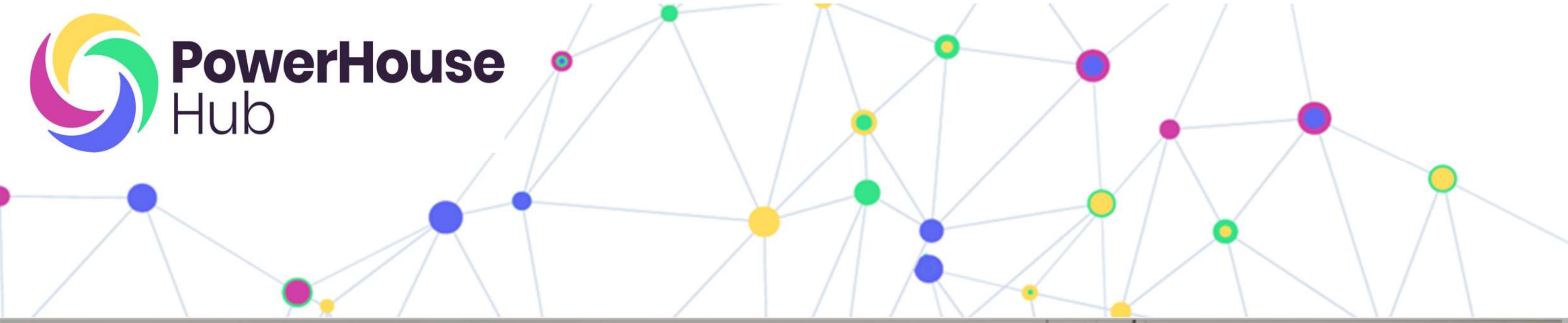

PowerHouse Hub

Data and Information Security Policy

Version 2023.4

Version Information

Version	**Date**	**Update**	**Author / Reviewers**	**Approved by**
2021 V 2.05	April, 2021	Annual Review and update	Philip Gay, Network Admin	Tony Carrucan, CEO
2023	Feb, 2023	Annual Review and update	Philip Gay, Network Admin	Tony Carrucan, CEO
2023.4	April, 2023	Additional updates	Philip Gay, Network Admin	Tony Carrucan, CEO

Contents

SOC2 Policies

Additional policies, practices and workflows that relate to PowerHouse Hub's SOC2 include:

- PowerHouse Hub System Architecture and Back-up
- PowerHouse Hub Incident Response Plan Reiterative Cycle
- PowerHouse Hub Privacy and Data Management
- PowerHouse Hub Configuration Controls
- PowerHouse Hub Service Level Agreement

PowerHouse Hub Network Security Policy

Password Policy

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 PowerHouse Hub's entire corporate network. As such, all PowerHouse Hub employees (including contractors and vendors with access to PowerHouse Hub systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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.

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 PowerHouse Hub facility, has access to the PowerHouse Hub network, or stores any non-public PowerHouse Hub information.

Policy

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 and system-level passwords must be stored in a password vault.
- All production system-level passwords must be part of the PowerHouse Hub administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" 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.

Guidelines

General Password Construction Guidelines

Passwords are used for various purposes at PowerHouse Hub. 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.
- 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.

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.
- 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 either of these examples as passwords!

Password Protection Standards

Do not use the same password for PowerHouse Hub accounts as for other non-PowerHouse Hub access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various PowerHouse Hub access needs. For example, select one password for the computer systems and a separate password for applications. Also, select a separate password to be used for an NT account and a UNIX account.

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

Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications should:

- support authentication of individual users, not groups.
- not store passwords in clear text or in any easily reversible form.
- 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.
- support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Use of Passwords and Passphrases for Remote Access Users

Access to the PowerHouse Hub Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
All of the rules above that apply to passwords apply to passphrases.

Enforcement

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

Wireless Communication Policy

Purpose

This policy prohibits access to PowerHouse Hub networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by our technical team are approved for connectivity to PowerHouse Hub's networks.

Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, smartphones, tablets, iPhones and iPads, etc.) connected to any of PowerHouse Hub's internal networks. This includes any form of wireless communication device capable of transmitting packet data.

Policy

To comply with this policy, wireless implementations must: Maintain point to point hardware encryption of at least 56 bits. Maintain a hardware address that can be registered and tracked, i.e., a MAC address.

Enforcement

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

Information Sensitivity Policy

Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of PowerHouse Hub without proper authorisation.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarise themselves with the information labelling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect PowerHouse Hub Confidential information (e.g., PowerHouse Hub Confidential information should not be left unattended in conference rooms).

Scope

All PowerHouse Hub information is categorized into two main classifications:

- PowerHouse Hub Public
- PowerHouse Hub Confidential

PowerHouse Hub Public information is information that has been declared public knowledge by someone with the authority to do so and can freely be given to anyone without any possible damage to PowerHouse Hub Systems.

PowerHouse Hub Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in PowerHouse Hub Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of PowerHouse Hub Confidential information is "PowerHouse Hub Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to PowerHouse Hub by that company under non-disclosure agreements and other contracts.

Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into PowerHouse Hub's network to support our operations.

PowerHouse Hub personnel are encouraged to use common sense judgment in securing PowerHouse Hub Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as PowerHouse Hub Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the PowerHouse Hub Confidential information in question.

Minimal Sensitivity:

General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "PowerHouse Hub Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "PowerHouse Hub

Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, PowerHouse Hub information is presumed to be "PowerHouse Hub Confidential" unless expressly determined to be PowerHouse Hub Public information by a PowerHouse Hub employee with authority to do so.

Storage:

Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction:

Deposit outdated paper information in specially marked disposal bins on PowerHouse Hub premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure:
Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

More Sensitive:

Business, financial, technical, and most personnel information.

Marking guidelines for information in hardcopy or electronic form.
Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".
As the sensitivity level of the information increases, you may, in addition or instead of marking the information "PowerHouse Hub Confidential" or "PowerHouse Hub Proprietary", wish to label the information "PowerHouse Hub Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Storage:

Individual access controls are highly recommended for electronic information.

Disposal/Destruction:

In specially marked disposal bins on PowerHouse Hub premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure:
Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Most Sensitive:

Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.
Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

To indicate that PowerHouse Hub Confidential information is very sensitive, you may should label the information "PowerHouse Hub Internal: Registered and Restricted", "PowerHouse Hub Eyes Only", "PowerHouse Hub Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Confidential Information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Storage:

Individual access controls are very highly recommended for electronic information.

Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction:

Strongly Encouraged: In specially marked disposal bins on premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure:
Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Enforcement

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

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

- Always run the anti-virus software installed on your workstation; install anti-virus software updates as they become available.
- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with PowerHouse Hub's
- Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct USB sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a USB from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- New viruses are discovered almost every day. Periodically check the Anti-Virus Policy and this Recommended Processes list for updates.

Workflows and Guidelines for Client Data

PowerHouse Hub understands the critical importance of protecting client data and site access. We prepare for our incident response life cycle by implementing a high level of security on three levels, hardware, application and database. Our AWS data servers have ISO 27001 certification.

Client Data Security Best Practices

Client portals are protected with the following practices:

Identity Theft Protection

Identity theft refers to fraud that involves someone pretending to be someone else for their own gain. We apply the current best practice to protect your users' identity theft including:

- Encrypted user password in database with strong encryption technique such as Bcrypt and/or AES-256
- Use alpha numeric combination and case sensitive for user passwords.
- Minimalist approach in storing and displaying user private information.

Secure Access Policies

All users on your training website will be assigned the privileges based on their user level.

This protection provides security with regard to access to administration portal. Your site administrator will have the access rights to add or delete any additional administration accounts. These administration accounts can be set as administrators or editors. There is also the option for your administrator to create additional administration accounts and set permissions and access rights to various modules.

SSL Encryption and Certificates

The SSL certificates encrypt the data on the site. After the secure connection is made, the session key is used to encrypt all transmitted data. SSL allows sensitive information such as credit card numbers, private information and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text —leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.

SSL Certificates are provided free of charge and will be automatically enabled on all Powerhouse Hub portal URLs. In addition to this, clients utilizing custom domains will be assigned free SSL Certificates provided by LetsEncrypt.

Session Hijacking Protection

PowerHouse Hub uses file system-based tracking for all users' sessions to mitigate session hijacking and Cross-Server Scripting (XSS) potential. This means that every time a user logs on to your portal, it generates a new session value and stores the value in the database. On every page of training portal where authentication is required, the user session will be compared with the one stored in database. As the session is renewed, this guarantees a user dynamic session value, which makes it harder to duplicate or followed, thus providing a higher level of security for your organisation.

Defamation of Site Protection

PowerHouse Hub protects against defamation of the site by preventing unauthorised access to file servers. Our systems feature data validation on all forms and write access on files and folders permission (executable, read and write). The file upload directories has read / write access permissions to prevent malicious users from executing code remotely to gain access to the site.

Firewall Security

Firewalls provide a key layer of security and control all access to and from the server on designated ports, IP addresses and TCP and UDP layers. The firewall allows certain users from a range of IP addresses to make requests to a designated port on the server or alternatively from server to IP addresses.

Load Balancing

If your training portal is an enterprise solution with high volumes of traffic, PowerHouse Hub can provide access to load balancing technology for annual upgrade. Load balancing technology provides two identical servers that are configured with identical specification and capacity. With the layer technology, it automates the distribution of website traffic between both servers. With this technology, it is capable to serve millions of user with static HTML request. When it comes to database interaction, generating image, and streaming video we can provide high quality streamed traffic to your users.

SQL injection Protection

SQL injection is a form of attack on a database-driven web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL Injection is a very common attack on search forms, login forms and most forms that send requests to server to access the server database. PowerHouse Hub guards the input data submitted by user to eliminate unwanted code or SQL commands to be passed into the processing script. This is achieved by including all permissible file extensions (i.e. PDF, jpeg, js) and block all scripting type statements and non-approved file extensions.

Security Organisation and Policy

Our company does not outsource information system functions as these are all completed by our programmers and developers on site in Australia and the United Kingdom.

PowerHouse Hub conducts personal screening for all of our employees (we do not engage contractors in this area of client security) involved in the administration of customer systems. The employee is initially screened with an Internet and social network filter. The employee must provide up to 3 referees and our HR department contact all referees as part of an extensive review of performance, risk, fraud, management). The employee must then present their government (ABN or company number) ID and/or passport to validate. Police criminal checks are also processed on employees with access to client files.

A formal part of our structured training for the team includes training on latest vulnerabilities and threats that relate to technologies that make up our stack. Security is also a standard agenda item on all stand-up and production meetings. With each new version release of our software we sponsor an independent Penetration Testing from an ethical hacking organisation. This allows us to document and address all know risks and submit the fixes back reiterative re-testing.

Customer Data Security

Our Lead Systems Architect/Engineer is vested with the sole rights of managing data on live sites. This data management is processed in accordance with strict access guidelines and documentation. The Lead Systems Architect has access to data on the Production Server. When a support ticket is issued, programmers liaise with the System Architect regarding access or issues with client data.

When establishing web service integration with a client's payroll, HRIS or existing database, PowerHouse Hub recommends a one-way data transaction process. The one-way process involves the client's database (i.e. Payroll), making specified dataset calls to the PowerHouse Hub Learning Management System (LMS) database. The LMS is the child to the parent (client) database. The dataset calls are established to be real-time calls or batched calls where data is written from the LMS to the Payroll system at midnight. PowerHouse Hub does not have access to a client's data and the data calls manage the transfer of data.

Client data on the Production server is managed by the client. PowerHouse Hub requires express written permission from the client to access the database for a specific purpose. For instance, responding to a support issue where PowerHouse Hub has been asked to investigate the records of a specific user. All requests are documented in our Zendesk helpdesk which delivers automated responses to the client. The support tickets are automatically written to our CRM and recorded against the client file. The production server has been optimised to ensure that all access to the client database is recorded automatically in the server logs which are reviewed daily by the Lead Systems Architect

We recommend that our clients do not include personal identifiable data on the development server which is used as the staging platform the creation of their site. After approvals the development site is duplicated and added to the Production Server. There is the option (recommended) for the client to purchase and PowerHouse Hub applies an SSL certificate to the site. The client then authorises in writing PowerHouse Hub to upload datasets to the live server.

The data can only be uploaded by the Lead Developer and all uploads are documented automatically in server logs, as do all access events on the server. After upload, all external sources of the data are deleted as part of the install process. Typically clients will upload their own data (via CSV, XML) import, LDAP, SSO, APIs or webservice calls. The production team do not have access to the live database unless it is needed to transact workflows documented in the Service Level Agreement. All requests must be approved and completed by the Lead Developer. At termination, our agreement provides explicit processes regarding the timely deletion of all client data. Termination clauses also facilitate the process where PowerHouse Hub will, under explicit written instructions, download the data and provide the data in a format that is reusable by the client.

All client data is categorised as Most Sensitive and the protocols outlined in the *Information Sensitivity Policy* section of this document. As such any data that relates to the client gathered during the development phase is destroyed accordingly.

Privacy Legislation and Client Data

The following information is included in the Standard Service Level Agreement which applies to all client projects (Refer to the PowerHouse Customer Agreement for GDPR compliance):

i. PowerHouse Hub must comply with the Privacy Act in relation to the Personal Information, whether or not PowerHouse Hub is an organisation bound by the Privacy Act in so far as they apply to PowerHouse Hub and/or the Services.

ii. PowerHouse Hub must:

a. use the Personal Information only for the permitted purposes of it carrying out its obligations under this Agreement;

b. not disclose Personal Information without the prior consent of the Customer except to an employee of PowerHouse Hub to the extent necessary for the permitted purposes of it carrying out its obligations under this Agreement or as required by law.

c. ensure that any person to whom Personal Information is disclosed as required by law, does not do or omit to do anything which, if done or omitted to be done by PowerHouse Hub, would constitute a breach of this clause;

d. obtain from any contractor of PowerHouse Hub to whom information is disclosed under as required by law, written agreement to comply with provisions having the same effect as this clause; and

e. not do anything or omit to do anything with the Personal Information that will cause the Customer to breach its obligations under the Privacy Act.

iii. PowerHouse Hub must not transfer Personal Information to a person (including itself) in a foreign country without the Customer’s prior written consent.

Please reference the PowerHouse Hub Customer Agreement and Service Level Agreement that outlines intellectual property ownership, obligations, GDPR compliance, warranties and response times.