

Policy and procedure management

ASSIGNMENT TWO



October 14, 2020

JAMIE LU

W0441213

Table of Contents

[INTRODUCTION: 3](#_Toc53609830)

[SECURITY PASSWORDS: 3](#_Toc53609831)

[1.0 Purpose 3](#_Toc53609832)

[2.0 Scope 4](#_Toc53609833)

[3.0 Statement of Guidelines 4](#_Toc53609834)

[4.0 Policy 4](#_Toc53609835)

[4.1 Password Creation 4](#_Toc53609836)

[4.2 Password Change 5](#_Toc53609837)

[4.3 Password Protection 5](#_Toc53609838)

[4.4 Application Development 5](#_Toc53609839)

[4.5 Multi-Factor Authentication 5](#_Toc53609840)

[5.0 Revision History 5](#_Toc53609841)

[Version 6](#_Toc53609842)

[Date of Change 6](#_Toc53609843)

[Responsible 6](#_Toc53609844)

[Summary of Change 6](#_Toc53609845)

[1.0 6](#_Toc53609846)

[October 2020 6](#_Toc53609847)

[Jamie Lu 6](#_Toc53609848)

[Initial version 6](#_Toc53609849)

[SECURITY USER ACCESS RIGHTS: 6](#_Toc53609850)

[1.0 Purpose 7](#_Toc53609851)

[2.0 Scope 7](#_Toc53609852)

[3.0 Policy Statement 7](#_Toc53609853)

[3.1 User Access Management 7](#_Toc53609854)

[3.2 User Registration 8](#_Toc53609855)

[3.3 User Responsibilities 8](#_Toc53609856)

[3.4 Network Access Control 8](#_Toc53609857)

[3.5 User Authentication for External Connections 9](#_Toc53609858)

[3.6 Supplier’s Remote Access to the Council Network 9](#_Toc53609859)

[3.7 Operating System Access Control 9](#_Toc53609860)

[3.8 Application and Information Access 9](#_Toc53609861)

[4.0 Revision History 10](#_Toc53609862)

[DISASTER RECOVERY: 10](#_Toc53609863)

[1.0 Purpose 11](#_Toc53609864)

[2.0 Scope 11](#_Toc53609865)

[3.0 Policy 11](#_Toc53609866)

[3.1 Contingency Plans 11](#_Toc53609867)

[4.0 Revision History 11](#_Toc53609868)

[WEB APPLICATION SECURITY POLICY: 12](#_Toc53609869)

[1.0 Purpose 13](#_Toc53609870)

[2.0 Scope 13](#_Toc53609871)

[3.0 Policy 13](#_Toc53609872)

[3.1 Web applications are subject to security assessments based on the following criteria: 13](#_Toc53609873)

[3.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. 14](#_Toc53609874)

[3.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments. 14](#_Toc53609875)

[3.4 The current approved web application security assessment tools in use which will be used for testing are: 14](#_Toc53609876)

[4.0 Revision History 14](#_Toc53609877)

[DATA BREACH RESPONSE POLICY: 15](#_Toc53609878)

[1.0 Purpose 15](#_Toc53609879)

[2.0 Scope 16](#_Toc53609880)

[3.0 Policy Confirmed theft, data breach or exposure of Health Data Systems Inc. (HDS) Protected data or Health Data Systems Inc. (HDS) Sensitive data 16](#_Toc53609881)

[Work with Forensic Investigators 17](#_Toc53609882)

[Develop a communication plan. 17](#_Toc53609883)

[3.2 Ownership and Responsibilities 17](#_Toc53609884)

[4.0 Revision History 17](#_Toc53609885)

[References 18](#_Toc53609886)

# INTRODUCTION:

This document serves as a continuation to the new ER Registration System project for Health Data Systems Inc. (HDS). This is a policy and procedure document. It contains the security passwords, security user access rights, disaster recovery, web application security, and data breach response system policies for the system.

# SECURITY PASSWORDS:

## 1.0 Purpose

The purpose of this policy is to provide the best practices for the creation of strong passwords, as well as establish a standard for the creation and the protection of those passwords.

## 2.0 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 Health Data Systems Inc. (HDS) facility, has access to the Health Data Systems Inc. (HDS) network, or stores any non-public Health Data Systems Inc. (HDS) information. It applies to all employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. The password guidelines apply to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

## 3.0 Statement of Guidelines

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “It’s time for vacation” or “block-curious-sunny-leaves”. Passphrases are both easy to remember and type yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

• Contain eight characters or less.

• Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

• Are some version of “Welcome123” “Password123” “Changeme123”

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

## 4.0 Policy

### 4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

4.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

4.1.3 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 to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

### 4.2 Password Change

4.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

4.2.2 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

### 4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Health Data Systems Inc. (HDS) information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3 Passwords may be stored only in “password managers” authorized by the organization.

4.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

### 4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must 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.

### 4.5 Multi-Factor Authentication

4.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

## 5.0 Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of Change | Responsible | Summary of Change |
| 1.0 | October 2020 | Jamie Lu | Initial version |
|  |  |  |  |

# SECURITY USER ACCESS RIGHTS:

## 1.0 Purpose

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important, valuable asset of Health Data Systems Inc. (HDS) which must be managed with care. All information has a value to the Council. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

## 2.0 Scope

This policy applies to all Health Data Systems Inc. (HDS) Councillors, Committees, Departments, Partners, Employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to Health Data Systems Inc. (HDS) information and information systems.

## 3.0 Policy Statement

Health Data Systems Inc. (HDS) will establish specific requirements for protecting information and information systems against unauthorised access.

Health Data Systems Inc. (HDS) will effectively communicate the need for information and information system access control.

### 3.1 User Access Management

Formal user access control procedures must be documented, implemented, and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by Health Data Systems Inc. (HDS). Each user must be allocated access rights and permissions to computer systems and data that:

• Are commensurate with the tasks they are expected to perform.

• Have a unique login that is not shared with or disclosed to any other user.

• Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

### 3.2 User Registration

A request for access to the Council’s computer systems must first be submitted to the HDS Information Services Helpdesk for approval. Applications for access must only be submitted if approval has been gained from the line manager.

When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee’s last working day. It is the responsibility of the line manager to request the suspension of the access rights via the HDS Information Services Helpdesk.

### 3.3 User Responsibilities

It is a user’s responsibility to prevent their userID and password being used to gain unauthorised access to Council systems by:

• Following the Password Policy Statements outlined above in Section 6.

• Ensuring that any PC they are using that is left unattended is locked or logged out.

• Leaving nothing on display that may contain access information such as login names and passwords.

• Informing HDS Information Services Helpdesk and the line manager of any changes to their role and access requirements.

### 3.4 Network Access Control

The use of modems on non-Council owned PC’s connected to the Council’s network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from Information Services before connecting any equipment to the Council’s network.

### 3.5 User Authentication for External Connections

Where remote access to the Health Data Systems Inc. (HDS) network is required, an application must be made via the IT Helpdesk. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a security question.

### 3.6 Supplier’s Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council’s network without permission from IT Helpdesk. Any changes to supplier’s connections must be immediately sent to the IT Helpdesk so that access can be updated or ceased. All permissions and access methods must be controlled by IT Helpdesk.

Partners or 3rd party suppliers must contact the IT Helpdesk before connecting to the Health Data Systems Inc. (HDS) network and a log of activity must be maintained. Remote access software must be disabled when not in use.

### 3.7 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) above must be applied. The login procedure must also be protected by:

• Not displaying any previous login information e.g. username.

• Limiting the number of unsuccessful attempts and locking the account if exceeded.

• The password characters being hidden by symbols.

• Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

### 3.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The IT Helpdesk of the software application is responsible for granting access to the information within the system. The access must:

• Be compliant with the User Access Management section (section 7.1) and the Password section (section 6) above.

• Be separated into clearly defined roles.

• Give the appropriate level of access required for the role of the user.

• Be unable to be overridden (with the admin settings removed or hidden from the user).

• Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.

• Be logged and auditable.

## 4.0 Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of Change | Responsible | Summary of Change |
| 1.0 | October 2020 | Jamie Lu | Initial version |
|  |  |  |  |

# DISASTER RECOVERY:

## 1.0 Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by Health Data Systems Inc. (HDS) that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

## 2.0 Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested, and kept up to date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

## 3.0 Policy

### 3.1 Contingency Plans

The following contingency plans must be created:

• Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?

• Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.

• Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.

• Criticality of Service List: List all the services provided and their order of importance.

• It also explains the order of recovery in both short-term and long-term timeframes.

• Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.

• Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

• Mass Media Management: Who oversees giving information to the mass media?

• Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Tabletop exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

## 4.0 Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of Change | Responsible | Summary of Change |
| 1.0 | October 2020 | Jamie Lu | Initial version |
|  |  |  |  |

# WEB APPLICATION SECURITY POLICY:

## 1.0 Purpose

The purpose of this policy is to define web application security assessments within Health Data Systems Inc. (HDS). Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Health Data Systems Inc. (HDS) services available both internally and externally as well as satisfy compliance with any relevant policies in place.

## 2.0 Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Health Data Systems Inc. (HDS).

All web application security assessments will be performed by delegated security personnel either employed or contracted by Health Data Systems Inc. (HDS). All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of Health Data Systems Inc. (HDS) is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

## 3.0 Policy

### 3.1 Web applications are subject to security assessments based on the following criteria:

a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

3.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

a) High – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

b) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

c) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

### 3.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

b) Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

c) Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

### 3.4 The current approved web application security assessment tools in use which will be used for testing are:

• Grabber

• Vega

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

## 4.0 Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of Change | Responsible | Summary of Change |
| 1.0 | October 2020 | Jamie Lu | Initial version |
|  |  |  |  |

# DATA BREACH RESPONSE POLICY:

## 1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Health Data Systems Inc. (HDS) Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how Health Data Systems Inc. (HDS)’s established culture of openness, trust and integrity should respond to such activity. Health Data Systems Inc. (HDS) Information Security is committed to protecting Health Data Systems Inc. (HDS)'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

## 2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Health Data Systems Inc. (HDS) members. Any agreements with vendors will contain language similar that protects the fund.

## 3.0 Policy Confirmed theft, data breach or exposure of Health Data Systems Inc. (HDS) Protected data or Health Data Systems Inc. (HDS) Sensitive data

As soon as a theft, data breach or exposure containing Health Data Systems Inc. (HDS) Protected data or Health Data Systems Inc. (HDS) Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

• IT Infrastructure

• IT Applications

• Finance (if applicable)

• Legal

• Communications

• Member Services (if Member data is affected)

• Human Resources

• The affected unit or department that uses the involved system or output or whose data may have been breached or exposed

• Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of Health Data Systems Inc. (HDS) data

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

### Work with Forensic Investigators

As provided by Health Data Systems Inc. (HDS) cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

### Develop a communication plan.

Work with Health Data Systems Inc. (HDS) communications, legal and human resource departments to decide how to communicate the breach to:

a) internal employees

b) the public

c) those directly affected

## 3.2 Ownership and Responsibilities

Roles & Responsibilities:

• Sponsors - Sponsors are those members of the Health Data Systems Inc. (HDS) community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Health Data Systems Inc. (HDS) Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

• Information Security Administrator is that member of the Health Data Systems Inc. (HDS) community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

• Users include virtually all members of the Health Data Systems Inc. (HDS) community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

• The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

## 4.0 Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of Change | Responsible | Summary of Change |
| 1.0 | October 2020 | Jamie Lu | Initial version |
|  |  |  |  |

# References

G3C Toolkit. (n.d.). *West Midlands ICT Policy Pack*. Retrieved October 14, 2020, from G3C Toolkit: http://g3ctoolkit.net.s3-website-us-west-2.amazonaws.com/ia/SecPol/wmspDownloads/IT\_Access\_Policy.doc

SANS. (n.d.). *Security Policy Templates*. Retrieved October 14, 2020, from SANS: https://www.sans.org/information-security-policy/?category=application-security,general,server-security,network-security,retired