Security Passwords

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Halifax Regional Hospital, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

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

3. 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 Halifax Regional Hospital facility, has access to the Halifax Regional Hospital network, or stores any non-public Halifax Regional Hospital information.

4. 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.

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. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

- Password Construction Guidelines

7. Revision History

Date of Change	Responsible	Summary of Change
October 2021	HRH Policy Team	Updated and converted to new format

Security User Access Rights

1. Overview

This policy is to provide a framework for how user accounts and privileges are created, managed, and deleted. It includes how new users are authorized and granted appropriate privileges, as well as how these are reviewed and revoked when necessary and includes appropriate controls to prevent users obtaining unauthorized privileges or access.

2. Purpose

The purpose of this policy is to support the Information Security Policy and provide a framework for the management of user access Halifax Regional Hospital information systems, networks, and equipment. These rules are in place to protect the employee and Halifax Regional Hospital.

3. Scope

This policy applies to:

- All employees and suppliers who have access to the Halifax Regional Hospital information and information systems.
- Information systems and services in program, project, and operational business areas.

There are some access roles which require implementing stronger controls than those for standard users.

4. Policy

4.1 Principle of Least Privilege

Access controls must be allocated on the basis of business need and 'Least Privilege'. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information, and resources that they need to fulfil their business role.

4.2 User Access Account Management

User account management procedures must be implemented for user registration, modification, and de-registration on all Halifax Regional Hospital information systems. These procedures must also include processes for monitoring redundant and inactive accounts. All additions, deletions, suspensions, and modifications to user accesses should be captured in an audit log showing who took the action and when. These procedures shall be implemented only by suitably trained and authorized employees. Access control standards must be established for all information systems, at an appropriate level for each system, which minimizes information security risks yet allows the organization's business activities to be carried out without undue hindrance. A review period

will be determined for each information system and access control standards will be reviewed regularly at those intervals. All access to Halifax Regional Hospital information systems must be controlled by an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user's identity. Users will normally be limited to only one user account for each individual information system for non-administrative purposes. Any variations from this policy must be authorized by the Senior Responsible Owner (SRO) or, where applicable, the Authority. All users shall have a user ID for their sole use for access to all computing services. All individual user IDs must be unique for each user and never duplicated. All user accounts that have not been accessed for an agreed period, without prior arrangement, must be automatically disabled. All administrator and privileged user accounts must be based upon job function and authorized by the SRO or, where applicable, the Authority, prior to access being given. All changes to privileged accounts must be logged and regularly reviewed. Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organization. Users' access rights will be reviewed at regular intervals no longer than annually. Access to systems by individual users must be authorized by their manager or where applicable, the Authority.

4.3 Password Management

Passwords must not be shared with any other person for any reason. All default system and vendor passwords must be changed immediately following installation. All Halifax Regional Hospital information systems must support strong password management techniques (such as: length, complexity, aging, history, account lockout). All Halifax Regional Hospital information systems must technically force new user accounts to change the initial password upon first use to a strong password and thereafter on a regular basis.

4.4 Monitoring User Access

Systems will be capable of logging events that have a relevance to potential breaches of security. User access will be subject to management checks.

4.5 Responsibilities

4.5.1 Senior Responsible Owner (SRO)

SROs are responsible for ensuring that the requirements of this policy are implemented within any program, projects, systems, or services for which they are responsible. The SRO is responsible for ensuring that a robust checking regime is in place and complied with to ensure that legitimate user access is not abused. The SRO may delegate responsibility for the implementation of the policy but retains ultimate accountability for the policy and associated checking regime. Any non-compliance with this policy must be supported by a documented and evidence-based risk decision accepted by the SRO.

4.5.2 Managers

Managers are responsible for ensuring that members of their team have the minimum levels of access to systems they need to perform their job. They must authorize the access rights for each individual team member and keep a record of the latest access permissions authorized. Managers should ensure that the access rights of people who have a change of duties or job roles or left the organization are revoked immediately and that any access tokens (smartcard/USB dongle) are recovered. All Managers should review the access levels of their people to ensure they are appropriate.

4.5.3 IT Support Teams

IT Support Teams are responsible for granting access to systems as described in local work instructions or use of Role Based Access Controls Matrix in accordance with the relevant procedures. IT Support Teams must evaluate and, if necessary, challenge authorized access to help identify any obvious anomalies in the access levels granted or requested.

4.5.4 Users

Users must only use business systems for legitimate use as required by their job and in accordance with the procedures for those systems.

5. Policy Compliance

Compliance against this policy will be assessed regularly. Any violation of this policy must be investigated and may result in disciplinary action being taken.

6. Definitions and Terms

6.1 Users

This is the collective term used to describe all those who have access to the Halifax Regional Hospital's information and information systems as outlined in the Scope of this policy.

6.2 Privileged Users

A privileged user is a user who has an elevated level of access to a network, computer system or application and is authorized to perform functions that standard users are not authorized to perform. This includes a "standard user" with approved elevated privileges that allows equivalent access to that of a privileged user

7. Revision History

Date of Change	Responsible	Summary of Change
October 2021	HRH Policy Team	Updated and converted to new format

Disaster Recovery

1. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives Health Data Systems Inc. a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

2. Purpose

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

3. 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.

4. Policy

4.1 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 is in charge of 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.

5. Policy Compliance

5.4 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.5 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.6 Non-Compliance

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

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

The following definition and terms can be found in the HRH Glossary located at:
https://www.hrh.ca/security-resources/glossary-of-terms/

- Disaster

8. Revision History

Date of Change	Responsible	Summary of Change
October 2021	HRH Policy Team	Updated and converted to new format.

Web Application Security Policy

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. Purpose

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

3. 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 Halifax Regional Hospital.

All web application security assessments will be performed by delegated security personnel either employed or contracted by Halifax Regional Hospital. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of Halifax Regional Hospital 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.

The new web application should leverage existing data being collected via web services (api - XML) currently available:

- **HBS (Heath Billing System)**
- **STAR (Patient Admission, Transfer and Discharge)**
- **HSM (Nursing software to determine patient procedures)**
- **PHS (Patient surgery scheduling)**

4. Policy

4.1 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.

4.2 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. HBS 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. HBS 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.

4.3 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.

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

- Tool/Abbey Scan
- Tool/AppTrana Website Security Scan
- Tool/ImmuniWeb

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.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

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

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

6 Definitions and Terms

None.

7 Revision History

Date of Change	Responsible	Summary of Change
October 2021	HRH Policy Team	Updated and converted to new format.

Remote Access Policy

1. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to Halifax Regional Hospital 's network from any host. These rules and requirements are designed to minimize the potential exposure to Halifax Regional Hospital from damages which may result from unauthorized use of Halifax Regional Hospital resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Halifax Regional Hospital internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all Halifax Regional Hospital employees, contractors, vendors, and agents with a Halifax Regional Hospital owned or personally owned computer or workstation used to connect to the Halifax Regional Hospital. network. This policy applies to remote access connections used to do work on behalf of Halifax Regional Hospital, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Halifax Regional Hospital networks.

4. Policy

It is the responsibility of Halifax Regional Hospital employees, contractors, vendors and agents with remote access privileges to Halifax Regional Hospital 's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Halifax Regional Hospital.

General access to the Internet for recreational use through the Halifax Regional Hospital network is strictly limited to Halifax Regional Hospital employees, contractors, vendors, and agents (hereafter referred to as "Authorized Users"). When accessing the Halifax Regional Hospital network from a personal computer, Authorized Users are responsible for preventing access to any Halifax Regional Hospital computer resources or data by non-Authorized Users. Performance of illegal activities through the Halifax Regional Hospital network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

Authorized Users will not use Halifax Regional Hospital networks to access the Internet for outside business interests. **But Hospital Admin staff should have VPN access to the Halifax Regional Hospital networks to access the Internet from outside during the period. (i.e., the time of Covid-19)**

For additional information regarding Halifax Regional Hospital 's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (Halifax Regional Hospital url).

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a Halifax Regional Hospital-owned computer to remotely connect to Halifax Regional Hospital 's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct Halifax Regional Hospital business must be approved in advance by InfoSec and the appropriate business unit manager.

4.1.5 All hosts that are connected to Halifax Regional Hospital internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.

4.1.6 Personal equipment used to connect to Halifax Regional Hospital 's networks must meet the requirements of Halifax Regional Hospital-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to Halifax Regional Hospital Networks*.

5. Policy Compliance

7.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

7.2 Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

7.3 Non-Compliance

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

6. Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Halifax Regional Hospital's network:

- *Security Password Policy*
- *Third Party Agreement*
- *Hardware and Software Configuration Standards for Remote Access to Health Data Systems Inc. Networks*

7. Revision History

Date of Change	**Responsible**	**Summary of Change**
October 2021	HRH Policy Team	Updated and converted to new format.