RISK PROFILE

INFORMATION MANAGEMENT/TECHNOLOGY – Systems/Technology Failure

Failure of critical biomedical technology, information systems, networks, hardware and communication technology can lead to unscheduled downtime, service interruptions, communication breakdown, missing important clinical information, productivity loss, excessive workload, etc. Technology failure can significantly compromise patient care and lead to patient safety issues.

This document contains information entered by HIROC Subscriber healthcare organizations (acute and non-acute) in the Risk Register application to help you in your assessment of this risk.

Key Controls / Mitigation Strategies

- Operational processes/technical controls:
  - ✓ Regular monitoring and updates to systems, software patches and security notifications
  - ✓ Hospital-wide patch management system, patching of most critical applications and equipment
  - ✓ Participate in regional cybersecurity committee, Regional Security Operations Centre
  - ✓ Regular preventative maintenance of all systems and equipment
  - ✓ Enroll corporate devices into device management system with encryption
  - ✓ Business impact identification and analysis of critical processes and applications
  - ✓ Virtual server management, firewall, anti-virus, spam filter, anti-malware, anti-spyware
  - ✓ Up to date firewalls, perform routine backups of firewalls, and vendor verified protection rules on Zero-Day Attacks
  - ✓ Spare firewall available to replace failed equipment
  - ✓ Network intrusion/threat detection systems in place
  - ✓ Server monitoring system to alert on common critical items
  - ✓ Develop policy and processes for acceptable downtime and backup/restore for critical applications
  - ✓ Industrial trended password policy, change your password policy
  - ✓ Define and implement Threat Risk Assessment (TRA) process, conduct initial TRA on critical assets
  - ✓ Assign controls and business owners on critical assets
  - ✓ Implement personal device compliance management tool
  - ✓ Sunset Terminal server/remote desktop access for external users
  - ✓ Multifactor authentication for external Virtual Desktop Infrastructure (VDI) access and external WebMail access, controlled external accesses

- Incident response/business continuity and recovery:
  - ✓ Regular backup of data, files, equipment and systems (e.g., offsite/offline tape and electronic backup solutions)
  - ✓ Encrypted USB for Electronic Medication Administration Record (eMAR) information
  - ✓ Third party hosted services (e.g., Tier 1 data centre)
  - ✓ Reduction of files stored in on-premises hardware and move files to Cloud environment for increased collaboration, ease of accessibility and increased security
  - ✓ Various system backup reduces Recovery Point Objective (RPO)
  - ✓ Local and external backups are verified. Multiple backups tested (local, onsite, offsite).
  - ✓ 24/7 network with third party vendor
  - ✓ Computers preprogrammed on a separate link, so the backup is always available to staff

RISK REGISTER

Date last reviewed: October, 2022

This is a resource for quality assurance and risk management purposes only, and is not intended to provide or replace legal or medical advice or reflect standards of care and/or standards of practice of a regulatory body. The information contained in this resource was deemed accurate at the time of publication, however, practices may change without notice

  - ✓ Manual backup system and processes in place
  - ✓ Comprehensive business continuity and disaster recovery plans in place for all systems
  - ✓ Define major incident response plan (Playbook), Cyber Security Plan, unplanned system downtime procedures
  - ✓ Embed a completed Business Continuity Plan (BCP) into Emergency Code response/Code grey protocols
  - ✓ Harmonization of all relevant policies and procedures with respect to downtime protocols and contingency planning
  - ✓ Routine data/system recovery drills, testing of plans
  - ✓ Create checklist and Standard Operating Procedures with specific operational instructions for all users
  - ✓ Establish recovery points and recovery time objectives
  - ✓ Disaster recovery site equipped with critical applications and services
  - ✓ Redundancy in power grid and backup generator, ensure critical systems/technology are connected to emergency power system
  - ✓ Redundancy in critical communication components, network and network switching technology
  - ✓ Back up mirrored copy of corporate documents
  - ✓ Redirect internet traffic through other provider and/or circuit
  - ✓ Land lines that analog phones can be connected to are available to allow calls in and out. Analog phone always active at reception.
  - ✓ Cell phones acquired with different provider

- Vendor management and third-party risks:
  - ✓ Vendor management program and contracts with emphasis on optimal operations/timely support intervention to avoid failures
  - ✓ Maintenance of medical devices and ensuring these devices (software and hardware) are upgraded by the third-party vendor in a timely manner
  - ✓ Reliable hosted services
  - ✓ Asking for security updates from external hosting companies
  - ✓ Cybersecurity insurance

- Awareness/education/training:
  - ✓ Education provided in general orientation
  - ✓ Mandatory annual privacy and cybersecurity training
  - ✓ Annual education presented to all departments. Inclusion of all staff, volunteers, students, and physicians.
  - ✓ Cybersecurity eLearning to address staff role in maintaining systems security
  - ✓ Conduct phishing campaigns to raise organizational awareness of threats of ransomware
  - ✓ Cyber Security Awareness Month
  - ✓ Regular acceptable and safe technology usage training, training on the use of technology policy
  - ✓ Staff awareness of emergency plan, including how and where to access it
  - ✓ Effective communication strategy to ensure business continuity and downtime protocols are well understood by appropriate personnel
  - ✓ Full cyber event response plan practice by the Emergency Operations Centre Team
  - ✓ Mock downtime exercises
  - ✓ Team attended a seminar regarding ransomware attacks

RISK REGISTER

Date last reviewed: October, 2022
This is a resource for quality assurance and risk management purposes only, and is not intended to provide or replace legal or medical advice or reflect standards of care and/or standards of practice of a regulatory body. The information contained in this resource was deemed accurate at the time of publication, however, practices may change without notice

INFORMATION MANAGEMENT/TECHNOLOGY – Systems/Technology Failure

- Strategic:
  - ✓ Manage multi-year refresh plan. Fulsome assets register to review age of equipment.
  - ✓ Capital planning to replace aging systems and invest in new technology
  - ✓ Execute on Strategic Roadmap to uplift current IT infrastructure and increase stability and security and improve collaboration across functions
  - ✓ Audit systems and make priority recommendations for capital purchase to support network system
  - ✓ Develop and execute a dedicated cyber strategy
  - ✓ Identifying multi-year cyber initiatives, roadmap
  - ✓ Define and approve cyber governance and operating model
  - ✓ External strategic partnerships (e.g., Ministry of Health, associations, community) on issues such as disaster recovery and common information systems/technology issues

Monitoring / Indicators

- Creating a schedule for review of servers
- Track all outages
- Unplanned system downtime, duration from down time start time until uptake of access to back up system
- Data/system recovery test results
- Obsolete systems and equipment still in use
- Internal and external system security audit results
- Automated network monitoring, system alerts of technology issues
- Monitors system performance in real-time
- Consistent monitoring of system for anomalies, bottlenecks, or signs of impending failure
- Staff complaints, IT ticket system tracks any issues submitted by front line users
- Review of incident reports
- Recalls and warnings
- Industry news, security reports, patch notifications, system updates
- Results of phishing tests, results of training
- Review of dashboard for antivirus software and backups, annual penetration testing
- Dashboard of compliance against patching
- Predictive analysis (e.g., when system will run out of space)
- Audit Departments to ensure they have downtime strategy
- Network traffic analyzer and bandwidth utilization

RISK REGISTER

Date last reviewed: October, 2022
This is a resource for quality assurance and risk management purposes only, and is not intended to provide or replace legal or medical advice or reflect standards of care and/or standards of practice of a regulatory body. The information contained in this resource was deemed accurate at the time of publication, however, practices may change without notice