GHS 2020 Information Technology Plan

Mission:

The GHS Information Technology team is dedicated in providing technology services that enable GHS to serve its mission and stakeholders in a secure and efficient technical environment. To accomplish this, we must transform the IT landscape at GHS while providing efficient and innovative IT services. Future trends for IT in primary and mental health care were explored revealing opportunities for innovation that will improve outcomes. GHS IT are dedicated to cyber security and keeping our systems safe. With new and developing threats, we continually update and assess the security of our network to protect and mitigate its impact.

Goals & Objectives:

Systems
- Transform and expand the data storage and network infrastructure to be more secure, scalable and responsive by utilizing cloud solutions where applicable.
- Implement next-generation technology to replace legacy systems.

Delivery
- Expand the clinical dashboard to increase productivity and lower administrative overhead with real-time costing.
- Improve the IT landscape through the development of governance and accountability.

Cybersecurity
- Become more proactive in responding to and detecting threats by deploying enhanced IT analytics and monitoring.
- Enhance cybersecurity tools and controls.

Culture
- Develop and maintain a skillful and motivated IT workforce to ensure future, sustainable success.
- Build relationships with similar organizations to collaborate and foster partnerships.

Training
- Provide multiple technology training initiatives.
- Increase awareness and understanding of security policies, threats and impacts.

Initiatives:

With technology changing quickly, we at GHS need to stay ahead of the curve. It seems like everything around us is connected to the Internet or some other network, so we will research and implement them, but also work to ensure they are secure. Upgrading legacy systems is important since most devices have a useful lifespan and if and when they expire, it creates a security risk because the manufacturer is no longer supporting it with updates, security patches, etc. We will continue our plan to replace older, outdated equipment and software, but add the need to include implementing next-generation technology. Other automation, such as an updated help request system, payroll system, and other customized web-based and mobile applications will be utilized as needed to improve productivity. We will continue to analyze how to utilize technology to improve our web site and increase visibility and availability to our stakeholders.

There has been a lot of talk about the “cloud” in recent years and questions about whether or not to move to it. We will explore the new opportunities that are present to make our computer infrastructure more
secure, and make it scalable so we are able to react to unforeseen circumstances and applications more easily. This should also help with our disaster recovery plan since the backing up and restoring data in one of the leading cloud services is reliable and responsive. Since we now are on a Multiprotocol Label Switching (MPLS) network with a fiber backbone, increasing our network bandwidth, we are able to fully utilize the benefits of the cloud and what it offers.

GHS utilizes a clinical dashboard developed in-house to lower administrative overhead and integrates financial information with real-time costing. We will expand this to include information for lower level management, as well as clinicians so they are able to see their pertinent data effortlessly at a glance.

The IT department strives to give the end users the service and delivery that is better than the industry standard. We will revamp how the help requests flow into the system to allow less issues to “fall into the cracks” and to be more responsive to staff. This should help with productivity as there should be less downtime for the end users.

Cybersecurity is more important than it has ever been in the past as there are many more threats out there designed to steal your money, intellectual property, personal information, etc. As security threats continue to grow, we face the challenge of protecting sensitive information on our GHS assets and applications. We have made several changes internally to combat this problem, but we need to go further to protect the agency against it. Malware is evolving and more sophisticated than ever, so we require the most advanced defenses to prevent and mitigate these types of cybersecurity attacks. We will implement and deploy next-generation technology to be proactive in detecting and mitigating vulnerabilities we encounter on a daily basis.

Attaining and maintaining skilled IT staff in the Flint area remains to be a challenge we face. Our goal is to keep our veteran staff, but also train our younger staff to ensure we are able to be viable in the future to meet the needs of our staff and providers. We will develop a training plan that includes mentorship and cross-training so we are not reliant on a particular staff and makes the entire team flexible. GHS IT is dedicated to developing our IT workforce’s technical competencies to reduce skill gaps and remain competitive in this dynamic environment.

After observing the big ransomware issue from our local county, it was found that we need to build relationships with more of the similar businesses around us. Collaborating and foster partnerships would allow us to trade ideas on what works, as well as assist each other if and when a disaster strikes. Shared resources could also be a benefit we should explore.

Several innovative training initiatives need to be made available to teach staff how to deal with malware, how to navigate the EMR proficiently, how to use the dashboard, etc. This will help GHS remain a leader in the mental health industry in Michigan by having a knowledgeable, but productive workforce. We will develop focused trainings to deal with the issues we are currently encountering.

Increase awareness and understanding of security policies is important because it helps keeping our computer infrastructure secure. We will launch a training and outreach campaign to educate the staff on current and potential cybersecurity threats and how to respond. It is each individual’s responsibility to be informed and empowered to assess and prevent potential threat situations.

Annually, the CIO will work with executive and other administrative staff and IT staff to evaluate current and future technology needs as they relate to the Agency’s strategic goals. The CIO will then determine technical budget needs for the following fiscal year for all technical financial accounts. Periodically throughout the year, the CIO will evaluate the status of these budget accounts and review remaining technical needs to ensure technical purchases needs meet expectations.
Policies:

- 04-001-01 Computer Information Systems
- 04-002-01 Computer Hardware Use
- 04-003-01 Computer Software Use
- 04-004-98 Integrity of Electronic Data
- 04-005-01 Information System Security
- 04-006-01 E-mail Use
- 04-007-01 Internet Use
- 04-008-11 Smart Phone Security policy
- 04-009-12 Mobile Phone Texting
- 04-010-14 Workstation Security
- 04-011-15 Sanction Policy
- 04-012-16 Security Management Policy
- 04-013-16 Security Workforce Policy
- 04-014-16 Information Access Management Policy
- 04-015-16 Security Awareness and Training Policy
- 04-016-18 Threat and Vulnerability Management Policy

Related Policies:

- 01-100-02 Corporate Compliance Program and Code of Conduct
- 04-101-02 HIPAA Privacy - Uses of Protected Health Information
- 04-103-02 HIPAA Privacy Disclosures of Protected Health Information