



IT & CyberSecurity Requirements for Facility Instruments		Element:	Standards and Guidelines
	IT SERVICES GEMINI OBSERVATORY	Document Number:	ITS-STG-001
		Revision:	1.2
		Creation Date:	09/07/2017
		Pages:	6

DESCRIPTION OF HISTORY / CHANGE
<p>Revision 0.1: 09/07/2017 - Document Initiated, Chris Morrison</p> <p>Revision 0.2: 11/24/2017 - Document Development, Chris Morrison, Andy Adamson</p> <p>Revision 1.0: 12/13/2017 - Final Document formatting, Chris Morrison</p> <p>Revision 1.1: 06/10/2019 - Document updates to include vendor details, Jose Varas</p> <p>Revision 1.2: 09/16/2019 - Document layout update to include header and version information, Chris Morrison</p>

APPROVAL SIGNATURE RECORD		
Reviewer Role	Title	Signature
Document Author	Gemini ISE	
Reviewer 1		
Reviewer 2		
Document Administrator	ITS Manager	
Approved by:	Gemini Deputy Director	
Accepted by:	Gemini Director	

IT & CyberSecurity Requirements for Facility Instruments		Element:	Standards and Guidelines
	IT SERVICES GEMINI OBSERVATORY	Document Number:	ITS-STG-001
		Revision:	1.2
		Creation Date:	09/07/2017
		Pages:	6

1. Purpose

Define and establish requirements for all the IT components and services that are installed within a facility instrument and that are required to maintain its operation and clarify the requirements to bring the instrument into an operational and sustainable model.

2. Scope

Given that each instrument is unique, it is understood that IT infrastructure will differentiate between each implementation. This requirements document, however, focuses on the general functionality of the IT infrastructure, how the components are identified and selected, how they are prepared and installed, and how they are eventually migrated from the development into the operations environment.


3. Definitions

The IT components include, but are not limited to the following:

- Computing hardware
- Storage requirements, both short and long-term
- Networking hardware and requirements
- Connectivity requirements such as cabling, internal and external port density etc.
- Operating system along with sustainability practices such as patching, updates etc.
- Configuration control
- Software and hardware interfaces that require access to services external to the instrument.

4. Introduction

Gemini maintains a set of standards covering computer hardware and operating systems, network hardware and connectivity, cybersecurity, and the sustainability of all IT components (including hardware and software). When a facility instrument is introduced into the Gemini operational IT infrastructure, meeting these requirements ensures its smooth integration and facilitates Gemini's ability to support the instrument throughout its lifecycle. into the future.

IT & CyberSecurity Requirements for Facility Instruments		Element:	Standards and Guidelines
	IT SERVICES GEMINI OBSERVATORY	Document Number:	ITS-STG-001
		Revision:	1.2
		Creation Date:	09/07/2017
		Pages:	6

5. Requirements


1) Computing Hardware

- a) For systems operating Linux or Windows, where possible, commercial off the shelf (COTS) DELL hardware should be purchased. We do not recommend using component built hardware.
- b) Wherever possible, and if the device only requires a network connection to maintain operations (no specialized connection cards within the device), all computer hardware should be installed in Gemini's datacenters.
- c) For rack servers, prefer high density over size. If the instrument requires many PCI cards, servers should be purchased in multiples of 2 Height Unit devices. (Instead of one 4HU device, purchase two 2HU devices).
- d) At least two exact copies of the computer hardware, including any purpose-specific cards that cannot be easily replaced with alternative brands or models, must be provided.
- e) If Apple hardware is required, the equipment must be purchased with AppleCare and the system must be able to be replaced within the Observatory defined hardware replacement cycle (end of AppleCare plus one year).
- f) If Dell hardware is required, the equipment must be purchased with warranty and support to include the minimum hardware lifecycle of three years (extended warranty and support contracts should be purchased if needed), and the system must be able to be replaced within the Observatory defined hardware replacement cycle (end of warranty plus one year).
- g) For Serial and/or Power Distribution inside the thermal enclosures, the Gemini Observatory prefers WTI units (Western Telematic, Inc.). Those units provide reach features including remote syslog logging for the serial ports, switched power sockets, remote access via HTTPS/SSH and more. Please consult with the Information Technology Services department (ITS) for supported models.


2) Local Storage

- a) All local storage should be provided on solid state devices (SSD)
- b) Each SSD must be delivered with an identical hardware backup unit.
- c) All local storage solutions should, at a minimum, be implemented as RAID 1
- d) In the interest of survivability and sustainability of systems and data, RAID 0 configurations are not permitted.


3) Centralized (Network) Storage

IT & CyberSecurity Requirements for Facility Instruments		Element:	Standards and Guidelines
	IT SERVICES GEMINI OBSERVATORY	Document Number:	ITS-STG-001
		Revision:	1.2
		Creation Date:	09/07/2017
		Pages:	6

- a) Prior to arrival at the telescope, the short-term storage requirements must be established to reserve space on the central network storage system or to expand the storage capacity as needed.
 - b) Long-term storage requirements must be established before the instrument enters official operations to clarify the expansion and budget requirements throughout the lifetime of the instrument.
- 4) Networking
- a) All network hardware must align with the Observatory’s networking infrastructure design, this includes the vendor (CISCO), operating system and feature set (such as 802.1x capabilities). The Information Technology Services department (ITS) shall provide the most up-to-date requirements as needed.
 - b) The instrument designer shall coordinate with the Gemini ITS department before purchasing any networking hardware.
 - c) All network hardware must be sustainable for the lifetime of the instrument.
 - d) Upon arrival to the telescope, all network management (usernames and passwords) must be handed to the Gemini ITS department, after which, periodic password updates will be coordinated.
 - e) If at all possible, using computers to establish the connectivity between two networks (essentially operating as a router) should be avoided. The Gemini ITS department can provide assistance to define a suitable sustainable solution.
 - f) The Gemini ITS department will provide a list of available IPv4 address ranges to be used by the instrument. The instrument builder should ensure that these addresses are configured and functional prior to shipping the instrument to Gemini. IPv6 is not supported.
- 5) Connectivity
- a) All communications to and from the instrument including any of its networked components (such as computers that are not physically installed within the instrument), must be clearly documented prior to arrival to the telescope.
 - b) All bandwidth and latency requirements must be understood and documented during the design phases of the instrument.
 - c) All connection requirements, including the amount of ports, port configuration (speed/duplex), form factor (LC fiber, RJ45 etc.) must be clearly documented.
 - d) All remote access requirements (including VPN access) for instrument staff to support the instrument at any point throughout its lifetime at Gemini, must be documented and approved by the Gemini ITS manager, prior to arrival to the telescope.
- 6) Operating Systems

IT & CyberSecurity Requirements for Facility Instruments		Element:	Standards and Guidelines
	IT SERVICES GEMINI OBSERVATORY	Document Number:	ITS-STG-001
		Revision:	1.2
		Creation Date:	09/07/2017
		Pages:	6

- a) CentOS compatible - Must be able to conform to Gemini Linux deployment and management procedures and standards (kickstart, spacewalk).
 - b) Windows 7/10 or Windows Server 2012/2016 are supported. If any other Windows operating system must be used, it must be justified and it is understood that Gemini ITS will implement safeguards to protect the Gemini IT infrastructure from any potential cybersecurity event.
 - c) macOS - Gemini ITS supports the current, plus the two previous releases of macOS. The system and configuration of it must conform to the macOS deployment and management procedures.
 - d) All systems must be upgradeable and patchable without affecting operations throughout the lifetime of the instrument.
 - e) All instrument-specific software must be designed to start up and shutdown properly using standard system conventions. i.e., if the host system is sent a shutdown command, the software should exit cleanly.
 - f) Gemini ITS department must be able to stop all system services, and remove all software that are not needed for operations (ie. Bluetooth, iSCSI, etc.) *without* affecting the functionality of the instrument, prior to the instrument entering operations.
- 7) Software Interfaces
- a) All pre-installed software and software licenses that are not required for the operation of the instrument, must be removed before the equipment is sent to Gemini.
- 8) Hardware Interfaces
- a) All fiber, Ethernet and any other IT specific connector form factor requirements (LC fiber, RJ45 etc.) must be clearly documented and communicated to the Gemini ITS department, before the instrument is sent to Gemini.
 - b) Multiport network cards should be used rather than configuring software virtual interfaces.
- 9) Backups
- a) Long term requirements for data backups must be documented
 - b) System backups - The procedure for generating and maintaining hot spares must be documented.
 - c) Source code that is required to build any hot spares, must be provided before the instrument is moved to operations.
- 10) Access control
- a) During testing and commissioning, it is acceptable for the instrument team to maintain privileged access.

IT & CyberSecurity Requirements for Facility Instruments		Element:	Standards and Guidelines
	IT SERVICES GEMINI OBSERVATORY	Document Number:	ITS-STG-001
		Revision:	1.2
		Creation Date:	09/07/2017
		Pages:	6

- b) Once the instrument is moved to operations, all privileged access accounts will be handed to the Gemini ITS department and the passwords will be modified. Provisions should be made by the instrument builder to ensure that doing so does not affect the operation of the instrument.