STANDARD SERIES

GLI-27:

Network Security Best Practices

Version 1.1

Revision Date: January 21, 2013

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

This Page Intentionally Left Blank

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved

ABOUT THIS DOCUMENT

This network security best practices resource has been produced by **Gaming Laboratories International, LLC** for the purpose of providing a "best practices" document specific to Network Security. Therefore, it is intended that this document be utilized as a reference for Network Security and not be viewed as a direct regulatory standard.

Network Security is a complex subject matter and varies widely as a function of the specific network and the type of data that is carried by that network. Additionally, the scale of the network often directly impacts the level and types of security measures implemented. For these reasons, the recommendations and guidance contained within this document should not be interpreted as being applicable to every network, as any one security element may or may not be suitable. Each network must be evaluated based on a number of factors such as those mentioned above, and then an appropriate plan developed for implementation. This document provides some level of guidance in terms of what best practices exist presently and how they might be applied to a given network. The information presented should therefore be viewed as offering considerations not requirements.

This Network Security best practices document is targeted to gaming regulatory agencies, gaming operators, and industry suppliers as a helpful reference for implementing network security measures. The document is in response to gaming industry stakeholders who have requested technical guidance in the network security space. It is not intended to represent a set of hard standards that every supplier and every network must comply with, as one size does not fit all in the network security space.

GLI-27 must be viewed as a living document which is expected to change as technology and network security practices evolve.

GLI-27 is not intended to replace or negate any current or future document in the GLI Standard Series. As just one example, the recommendations in GLI-27 are not intended to circumvent any specifications in GLI-21 should the network in question support Client Server functionality. Likewise for other types of networks and the GLI standards document that specifically applies to those networks.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved

This Page Intentionally Left Blank

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved

Table of Contents

CHAPTER 1 7

1.0 STANDARD OVERVIEW 7

1.1 Introduction 7
1.2 Acknowledgement of Other Documents Reviewed 8
1.3 Purpose of this Best Practices Reference 8
1.4 Principles of Secure Network Design 9
1.5 Key Network Security Definitions 10
1.6 Key Network operator / Stakeholder Documentation 16

CHAPTER 2 18

2.0 NETWORK HARDWARE 18

2.1 Networking Devices 18
2.2 Physical Access Controls and Security 21
2.3 Physical Ports and Wired Connections 22
2.4 Disaster Recovery and Redundancy (Physical) 23

CHAPTER 3 26

3.0 NETWORK SOFTWARE 26

3.1 Protocols and Communications 26
3.2 Firewalls 27
3.3 Password Protection and Logins 30
3.4 Multi-layered Protection 32
3.5 Encryption – Transmission and Storage 32
3.6 External Connections 37
3.7 Antivirus and Malware Protection Programs 39
3.8 Software Updates and Patches 39
3.9 Disaster Recovery (Logical) 40
3.10 Intrusion Detection and Prevention 41
3.11 Vulnerability Scanning 43
3.12 Logging 44
3.13 Remote Access 44

CHAPTER 4 46

4.0 WIRELESS NETWORKS 46

4.1 Industry Standards 46
4.2 Unique Considerations 46

CHAPTER 5 54

5.0 SOCIAL ENGINEERING AND EDUCATION 54

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

5.1 General Statement 54
5.2 Vendor Impersonations 54
5.3 Publicly Available Information 54
5.4 Voicemail Security 55
5.5 Targeted Email "Phishing" 55
5.6 Sensitive Document Disposal 55

CHAPTER 6 57

6.0 CLOUD COMPUTING RESOURCES 57

6.1 General Statement 57
6.2 General Considerations 57

APPENDIX 59

List of Figures 59

Figure 1 – Sample Topology for a Wired Network 59
Figure 2 - Topology for a Wireless Network 60

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

CHAPTER 1

1.0 STANDARD OVERVIEW

1.1 Introduction

1.1.1 ***General Statement***. **Gaming Laboratories International, LLC (GLI)** has been testing gaming equipment since 1989. Over the years, we have developed numerous standards for jurisdictions all over the world. GLI has chosen to create this document as a best practices resource for gaming regulatory agencies and gaming operators as a reference for implementing network security measures. In recent years, many gaming industry stakeholders have opted to ask for technical guidance in the network security space. In addition, network security technology is inherently complex so GLI realized the need to create a reference in a format familiar to the industry which can assist in building their knowledge of network security disciplines. This document, GLI Standard 27, will set forth the Best Practices in Network Security.

1.1.2 ***Document History***. This document is based upon industry examples of network security, and principally technical standards adopted by the State of Arizona as well as common requirements extracted from applicable standards defined by NIST and ISO. We have taken each of the standards' documents, merged each of the unique rules together, eliminating some rules and updating others, in order to reflect both the change in technology and the purpose of maintaining an objective, factual reference. We have listed below, and given credit to, agencies whose documents we reviewed prior to writing this best practices resource. It is the policy of **Gaming Laboratories International, LLC** to update this document as often as possible to reflect changes in technology, testing methods, or cheating methods. This document will be distributed FREE OF CHARGE to all those who request it. This reference and all others may be obtained by downloading it from our website at www.gaminglabs.com or by writing to us at:

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

Gaming Laboratories International, LLC
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

1.2 Acknowledgement of Other Documents Reviewed

1.2.1 ***General Statement***. These best practices have been developed by reviewing and using portions of the documents from the organizations listed below, where applicable. We acknowledge all that have assembled these documents and thank them:

a) National Institute of Standards and Technology (NIST) – Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53 Revision 2;
b) National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146
c) State of Arizona, Government Information Technology Agency (GITA) – Network Security, P800-S830 Rev 2.0;
d) International Standards Organization (ISO) International Electrotechnical Commission (IEC) 27002 and ISO IEC 27005; and
e) "All In One CISSP", CISSP Certification and Exam Guide, by Shon Harris.

1.3 Purpose of this Best Practices Reference

1.3.1 ***General Statement***. The Purpose of this Best Practices Reference is as follows:

a) To create a reference for gaming industry stakeholders interested in regulating, analyzing or certifying gaming networks.
b) To create a reference stakeholders can utilize to ensure the gaming network systems are secure and able to be audited and operated correctly.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

c) To construct a reference that can be easily changed or modified and allow for new technology to be introduced.

d) To construct a reference in a format familiar to gaming stakeholders which can better edify them on network security disciplines.

e) To construct a best practices resource that does not specify any particular method of network security. The intent is to allow a wide range of methods to be used to conform to the best practices, while at the same time, to encourage new methods to be developed.

1.3.2 ***No Limitation of Technology***. One should be cautioned that this document should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this best practices reference, make changes and incorporate accommodations for the new technology.

1.4 Principles of Secure Network Design

1.4.1 ***Network Security Design Principles***. Prior to implementing a network security solution, several key principles must be considered. Some of these principles include:

a) **Integrity** means that the security measures must be preservative. They must not corrupt data. They must not lose data. They must protect the data in a consistent way at all times. They must protect confidentiality and sensitivity of data.

b) **Availability** means that the security measures must be available at all times and that the systems and data they are protecting must be available at all times.

c) **Adequate protection** means that what you are protecting must be protected to a degree commensurate with their value. Computer items must be protected only until they lose their value and they must be protected to a degree consistent with their value.

d) **Effectiveness** means that any controls that are implemented must be effective in securing the network and its component parts. However, they must also be efficient, easy to use and appropriate to the size and type of organization in which they operate.

e) **Depth protection** means that it must be assumed that an intruder will attempt to use any available means of penetration. This does not necessarily entail the most obvious means,

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

nor is it necessarily the one against which the most solid defense has been installed.

f) **Due diligence** means that ensuring network security is an ongoing, evolving process. The network must be perpetually monitored and managed to ensure security.

1.5 Key Network Security Definitions

1.5.1 ***General Statement***. In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can further be defined by their topology or general configurations. Networks can also be characterized in terms of spatial distance as Local Area Networks (LANs), and Wide Area Networks (WANs). Further characterizations can be accomplished by referencing the type of data transmission technology in use; by whether it carries voice, data, or both kinds of signals; by users of the network; by the nature of its connections; and by the types of physical links.

1.5.2 ***Network Security Objectives.*** Network security equates to the protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and that all software on the network is an authentic copy of the original software as distributed by its manufacturer. Network security also helps to ensure the integrity of data that traverses the network.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

1.5.3 Definitions.

Term	Descriptions
Access –	Ability to make use of any information system (IS) resource.
Access Authority –	An entity responsible for monitoring and granting access privileges for other authorized entities.
Access Control –	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services specific to a network; and 2) to enter specific physical facilities which houses critical network infrastructure.
Adequate Security –	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Advanced Encryption Standard – (AES)	The Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.
Antivirus Software –	Software used to prevent, detect and remove computer viruses, including malware, worms and Trojan horses.
Application –	Computer Software designed to help a user perform a specific task.
Audit Data –	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Audit Trail –	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.
Authentication –	Verifying the identity of a user, process, software package, or device, often as a prerequisite to allowing access to resources in an information system.
Backup –	A copy of files and programs made to facilitate recovery if necessary.
Contingency Plan –	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
Data Integrity –	The property that data is both accurate and consistent and

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

Term	Descriptions
	has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
Demilitarized Zone – (DMZ)	A network inserted between a company's private network and the outside public network. Systems that are externally accessible but need some protections are usually located on DMZ networks.
Disaster Recovery Plan – (DRP)	A written plan for processing critical applications and preventing loss of data in the event of a major hardware or software failure or destruction of facilities.
Encrypted Key –	A cryptographic key that has been encrypted using an Approved security function with an encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext.
Encrypted Network –	A network on which messages are encrypted to prevent reading by unauthorized parties.
Encryption –	Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people.
Firewall –	A mechanism or device that limits access between networks in accordance with local security policy.
Honeypot –	A host that is designed as a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems and has no authorized users other than its administrators.
Incident –	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident Response Plan –	The documentation of a predetermined set of instructions or procedures when a malicious cyber attack is encountered against an organization's IT systems(s).
Intrusion Detection System – (IDS)	Software that looks for suspicious activity and alerts administrators.
Intrusion Prevention Systems –	Systems which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
IP Address –	An IP address is a unique number for a computer that is

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

Term	Descriptions
	used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.
IP Security – (IPSec)	IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec is an Institute of Electrical and Electronic Engineers (IEEE) standard, Request For Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect Virtual Private Network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol.
Kerberos -	A network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.
Key –	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.
Malware –	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Message Authentication Code – (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Non-repudiation –	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Password –	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

Term	Descriptions
	authorization.
Personal Identification Number – (PIN)	A password consisting only of decimal digits. A secret code that a claimant memorizes and uses to authenticate his or her identity. PINS are generally only decimal digits. An alphanumeric code or password used to authenticate an identity.
Phishing –	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
Policy (for Security) –	A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance
Port –	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).
Private Key –	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. **Asymmetric key** encryption uses different keys for encryption and decryption. These two keys are mathematically related and they form a key pair.
Proxy –	A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, an Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and an Simple Mail Transfer Protocol (SMTP) proxy used for e-mail.
Public Key –	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Remote Access –	Access by users (or information systems) communicating external to an information system security perimeter.
Risk–	The likelihood of a threat being successful in its attack against a network.
Secure Communication Protocol –	A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection.
Social Engineering –	An attempt to trick someone into revealing information

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

Term	Descriptions
	(e.g., a password) that can be used to attack systems or networks.
Threat –	Any circumstance or event with the potential to adversely impact network operations (including mission, functions, image, or reputation), assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. A threat is any potential danger to a network that someone or something may be able to identify as being vulnerable, and therefore seek to exploit.
Unauthorized Access –	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Verification and Validation	Ensuring by electronic signature checking that any software package is an authentic copy of the software created by its manufacturer and, if applicable, an exact copy of the software as certified by the ITL. Standards for verification and validation are addressed within other applicable GLI Standards.
Virtual LAN – (VLAN)	A Virtual LAN (VLAN) is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs are implemented by adding a header to each frame that contains "tags" to identify which LAN the frame belongs to.
Virtual Private Network – (VPN)	A Virtual Private Network is a logical network that is established over an existing physical network and which typically does not include every node present on the physical network.
Virus –	A self-replicating program, typically with malicious intent, that runs and spreads by modifying other programs or files.
Vulnerability –	Software, hardware, or other weaknesses in a network that can provide a "door" to introducing a threat.

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

1.6 Key Network operator / Stakeholder Documentation

1.6.1 ***Identification of Risk.*** There is no completely secure system. Therefore. It is necessary to define which portions of the business require the greatest resources targeted at security. Each discrete unit in an organization will have some portion of its core functionality dependent in information technology and should be an interested party. Each interested party should be able to define which specific functions are at risk from data loss, tampering, or leakage. This can be considered to be the first step in a risk analysis which should be used as a basis for the Information Security policies.

1.6.2 ***Information Security Policies (prevention).*** A detailed Security Policy (hereafter "the policy") is required to identify, document, and support the many facets of network security described throughout this document. Development of the policy should be predicated upon performance of a detailed risk analysis. The policy document should be developed, implemented, and maintained by the network operators / stakeholders and shall

a) Be formally documented and reviewed regularly.

b) Define employee expectations and responsibilities, and establish consequences for failure to follow policy, and additionally:

   i. Define roles and responsibilities within the organization for information security.

   ii. Set the vision of senior management in regards to security.

   iii. Define protection requirements in accordance with the risk assessment.

   iv. Incorporate employee awareness training, which should be done at time of hire and annually thereafter.

1.6.3 ***Incident Response Policy (response).*** An Incident Response Policy (IRP) is essential to ensuring that network security threats are responded to in a timely and effective manner should preventive measures fail or be compromised. A detailed IRP document should be developed, implemented, and maintained by the network operator / stakeholder and shall:

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

a) Be formally documented and tested annually.
b) Define roles and responsibilities during an incident.
c) Define a communication plan both internally and externally (media).

1.6.4 ***Disaster Recovery Plan (recovery).*** High-level practices and procedures should be established to help in the event of the failure of critical infrastructure, and to help control damage in the event that preventative network security measures are unsuccessful in warding off an attack. A detailed Disaster Recovery Plan (DRP) document should be developed, implemented, and maintained by the network operator / stakeholder and shall ensure that:

a) Personnel are trained and familiar with related procedures.
b) Data backups are performed and maintained and sent off-site at regular intervals (preferably daily).
c) Multiple data centers are designed into the network operations.
d) High availability systems are effectively utilized which keep both the data and system replicated off-site.

Special Note: *A Disaster Recovery Plan is viewed as the principal responsibility of the network operator versus something that a network supplier is accountable for. That said, any credible DRP should involve and utilize the specific expertise and knowledge that the network supplier has to offer. Additionally, not all networks warrant the development and maintenance of a formal DRP, since they may be small-scale, unsophisticated networks that carry data of low sensitivity. Network operator internal controls should dictate the necessity for a DRP subject to the type of network in use and the nature of the data that is transmitted over that network.*

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

CHAPTER 2

2.0 NETWORK HARDWARE

2.1 Networking Devices

2.1.1 Types of Networking Devices. The table below briefly summarizes a variety of networking devices commonly used in modern-day networks.

TABLE 2.1.1 - NETWORKING DEVICES SUMMARY

Device	Function/Purpose	Key Points
Hub	Connects devices on a twisted-pair network.	A hub does not perform any tasks besides signal regeneration.
Switch	Connects devices on an 802.3 network.	A switch forwards data to its destination by using the MAC address embedded in each packet.
Bridge	Divides networks to reduce overall network traffic.	A bridge allows or prevents data from passing through it by reading the MAC address.
Router	Connects networks together.	A router uses the software-configured network address to make forwarding decisions.
Gateway	Translates from one data format to another.	Gateways can be hardware or software based. Any device that translates data formats is called a gateway.
Channel Services Unit / Digital Services Unit (CSU/DSU)	Translates digital signals used on a LAN to those used on a WAN.	CSU/DSU functionality is sometimes incorporated into other devices, such as a router with a WAN connection.
Network Interface Card (NIC)	Enables computer terminals and systems to connect to the network.	Network interfaces can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
Integrated Services Digital	Connects devices to ISDN lines.	ISDN is a digital WAN

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

Device	Function/Purpose	Key Points
Network (ISDN) terminal adapter		technology often used in place of slower modem links. ISDN terminal adapters are required to reformat the data format for transmission on ISDN links.
System area network card	Used in server clusters to provide connectivity between nodes.	System area network cards are high-performance devices capable of coping with the demands of clustering applications.
Wireless Access Point (WAP)	Provides network capabilities to wireless network devices.	A WAP is often used to connect to a wired network, thereby acting as a link between wired and wireless portions of the network.
Modem	Provides serial communication capabilities across phone lines.	Modems modulate the digital signal into analog at the sending end and perform the reverse function at the receiving end.

2.1.2 Key Networking Device Descriptions.

a) **Hubs:** Hubs are the simplest network devices and simply broadcast the same information to all connected ports including the originating port. On a hub, data is forwarded to all ports, regardless of whether the data is intended for the system connected to the port. Computers connect to a hub via a length of twisted-pair cabling. In addition to ports for connecting computers, most hubs have a port designated as an uplink port that enables the hub to be connected to another hub to create larger networks.

b) **Switches:** On the surface, a switch looks much like a hub. Multiple switches can be used, like hubs, to create larger networks. Despite their similarity in appearance and their identical physical connections to computers, switches offer significant operational advantages over hubs. Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected. It looks at the Media Access Control (MAC) addresses of the devices connected to it to determine

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

the correct port. A MAC address is a unique number that is programmed into every NIC. By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically. In effect, the switch channels or switches data between the ports.

c) **Bridges:** Bridges are networking devices that divide up networks. A bridge functions by blocking or forwarding data, based on the destination MAC address written into each frame of data. If the bridge believes the destination address is on a network other than that from which the data was received, it can forward the data to the other networks to which it is connected. If the address is not on the other side of the bridge, the data is blocked from passing. Bridges "learn" the MAC addresses of devices on connected networks by "listening" to network traffic and recording the network from which the traffic originates. The advantages of bridges are simple and significant. By preventing unnecessary traffic from crossing onto other network segments, a bridge can dramatically reduce the amount of network traffic on a segment. Bridges also make it possible to isolate a busy network from a not-so-busy one, thereby preventing pollution from busy nodes. When a Wireless Access Point allows communication between wireless clients and wired clients, then it is acting as a bridge between these networks.

d) **Routers:** Routers are network devices that literally route data among computer networks beyond directly connected devices. By examining data as it arrives, the router is able to determine the destination address for the data; then, by using tables of defined routes, the router determines the best way for the data to continue its journey. Unlike bridges and switches, which use the hardware-configured MAC address to determine the destination of the data, routers use the software-configured network address to make decisions.

e) **Gateways:** The term gateway is applied to any device, system, or software application that can perform the function of translating data from one format to another. The key feature of a gateway is that it converts the format of the data, not the data itself.

f) **Wireless Access Points (WAPs):** WAPs are hub-like devices, typically with a protruding antennae. They allow connectivity via an air interface. A WAP serves as a link between wired and wireless portions of a network.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

g) **Modems:** Modems perform a simple function: They translate digital signals from a computer into analog signals that can travel across conventional phone lines. The modem modulates the signal at the sending end and demodulates at the receiving end. Modems provide a relatively slow method of communication.

h) **Network Interface Cards (NICs):** Network Interface Cards (NICs), sometimes called simply network cards, are the mechanisms by which computers connect to a network.

2.2 Physical Access Controls and Security

2.2.1 ***General Statement***. Physical security equates to the ability to permit or deny the use of a particular resource by a particular entity through some physical or tangible means. Physical security is an important component of the protection of any network. Physical access controls are security features that control how users and systems communicate and interact with other systems and resources, and they serve to protect the systems and resources from unauthorized access. Physical network security should address the key areas of theft, sabotage, vandalism, accidents, and environmental and/or natural calamity.

2.2.2 ***Server Room Access***.

a) Unauthorized access to server rooms shall be prevented by the implementation of locked entry points and/or a swipe card system, or similar mechanism, capable of logging and/or controlling all entries to rooms in which systems hosting sensitive information are present. Some regulatory bodies require two factor authentication.

b) Logs shall be routinely reviewed for any anomalies in access patterns.

2.2.3 ***Server Rack/Cabinets Security***.

a) Server rack/cabinets shall be securely locked to create a physical barrier to accessing the servers.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

b) Access to server racks/cabinets shall be restricted to authorized employees only.

2.3 Physical Ports and Wired Connections

2.3.1 Network Jack Security.

a) Network jacks shall be disabled when not in use. This may be by :
b) Physical disconnection (air gap)
c) Administrative, such as assigning to a special "dead" VLAN
d) Installing a locked box or jack plug.
e) A log of enabled network jacks shall be maintained and audited regularly.
f) Requests and approvals for jack activations shall be logged by Information Technology (IT) staff.

2.3.2 Networking Devices.

a) Where networking devices are not in the server room,access to networking devices (routers, firewalls, switches, etc.) shall be restricted to authorized employees only.
b) Networking devices shall reside in a secure environment.

2.3.3 Unnecessary Service and Ports.

a) Networking devices shall have unnecessary/unused services turned off and non-essential ports disabled. (NOTE: The network supplier should be consulted prior to the deactivation of any services or ports to ensure that an essential service/port is not inadvertently disabled. For example, many essential services only run sporadically, so usage by itself is not always a reliable measure of importance.)

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

b) Proper design and build of the network shall be followed for all new network configurations to ensure that the appropriate security controls are implemented.

2.4 Disaster Recovery and Redundancy (Physical)

2.4.1 Disaster Recovery and Redundancy. Network redundancy involves making resources available in case of failure and making those resources available as seamlessly as possible and with little manual interaction in the event they are needed. Disaster recovery means having a plan in case of catastrophic failure to return access to resources quickly. The network shall utilize one or more of the following items to support disaster recovery and redundancy:

a) Redundant Hardware – The network shall utilize multiple pieces of hardware, such as NICs, that operate in parallel. In the event one fails, the other will continue to function.

b) High-Availability – The network shall employ multiple pieces of hardware, such as routers, that are identical, and configured in such a way that if the primary hardware component fails, the secondary one will take over with little or no administrative interaction.

c) Swappable Hardware / Cold Spares – Exact copies of hardware shall be maintained, such that in the event of a failure, that hardware can be readily swapped or replaced. This includes hardware that is not fully configured in a working capacity, but which can be taken from inventory, configured, and implemented in the network in fairly short order in the event of a component failure. This reduces or eliminates the downtime associated with repairing the original hardware component or acquiring and configuring a brand new replacement.

d) Mirroring – The network shall utilize mirroring. Mirroring typically applies to data storage and is the process of having all data, including changes, replicated to a second location in real-time. This replication process allows for either a hardware swap or the restoration of data in the event of a failure.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

e) Backup Data Centers – The network shall employ multiple data centers or sites – namely, a primary and secondary site. The secondary site can be utilized in the event of a major emergency and/or natural disaster or other calamity at the primary site.

i. Cold Backup Site – The least expensive but most time consuming. A Cold backup site is nothing more than an appropriately-configured space in a building. Everything required to restore network service must be procured and delivered.

ii. Warm Backup Site – A site already stocked with hardware representing a reasonable facsimile of that found at the primary site. Typically, the most recent data backups must be delivered and a restore must be performed.

iii. Hot Backup Site – The most expensive but quickest for recovery. A hot site generally contains a virtual mirror of the current site with systems essentially at-the-ready to be activated at a moment's notice.

With regards to Backup Data Centers, the term "site" may refer to physical space that is collocated or geographically separated. Geographic separation may offer the greatest security, redundancy, and survivability, but it also comes at the greatest expense. Therefore, this is a business decision that the network operator must evaluate in conjunction with the specific network and data involved.

2.4.2 ***Disaster Recovery Plan***. – As described earlier in this document, a Disaster Recovery Plan (DRP) shall carefully document all methods that are utilized to support disaster recovery of the network. This plan should also document essential contact information and should detail the required steps to affect a full recovery of the network. All key members and upper management should have multiple forms of access to the DRP document, both in electronic and printed form, and the plan should be reviewed frequently to address changes to sites, equipment, procedures, and personnel.

2.4.3 ***Network Backup***. The following items for information backup are required to ensure network security:

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

a) the necessary level of back-up information shall be defined and a disaster recovery plan documented;

b) accurate and complete records of the backup copies and documented restoration procedures shall be produced;

c) the extent (e.g. full or differential backup) and frequency of backups shall reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization;

d) the backups shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site but still retrievable in a timely manner to maintain data availability;

e) backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site shall be extended to cover the back-up site;

f) backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary;

g) restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;

h) in situations where confidentiality is of importance, backups shall be protected by means of encryption. While NIST does not specifically require backup encryption, they do maintain standards for encryption of data storage, and backup data may be viewed as an extension to that.

Special Note: *Disaster Recovery, a Disaster Recovery Plan, and Network Backup must be assessed in the context of the network in question. Some networks do not warrant one or more of these approaches. A proper risk analysis should be performed for the network in conjunction with a cost-benefit analysis to determine which approach is needed and to what extent it is financially prudent.*

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

CHAPTER 3

3.0 NETWORK SOFTWARE

3.1 Protocols and Communications

3.1.1 ***Network Protocols***. This section summarizes commonly-used networking protocols. The specific protocol that is appropriate for implementation in a given network is beyond the scope of this document. However, Transmission Control Protocol / Internet Protocol (TCP/IP) is a pervasive protocol used in the majority of modern-day networks.

a) UUCP (UNIX-to-UNIX Copy Protocol) – a set of Unix programs used for sending files between different Unix systems and for sending commands to be executed on another system.

b) TCP / UDP – Transport method protocols utilized as part of the TCP/IP protocol suite. TCP ensures that data arrives intact and complete, while UDP just sends out packet. TCP is used for everything that must arrive in perfect form and UDP is used for functions like streaming media and video conferencing where it is impossible to transmit erroneous or dropped packets.

c) SNMP (Simple Network Management Protocol) – A widely used network monitoring and control protocol that is part of the TCP/IP protocol suite. SNMP agents collect and analyze data that is passed to discover and analyze traffic patterns.

d) RMON (Remote Monitoring) – Enhancement to the SNMP protocol that adds a comprehensive set of network monitoring capabilities and allows for much more information about a network to be passed to a remote location.

e) DHCP (Dynamic Host Configuration Protocol) – A function in both software and the operating system of most hardware that allows for automatically assigned temporary IP addresses to be assigned on a request basis.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

f) FTP (File Transfer Protocol) - A widely used protocol for moving files across unknown or heterogeneous networks.

3.1.2 Secure Communications.

a) All confidential communications shall employ some form of encryption that has been approved by the network operators / stakeholders.

b) All confidential data communication shall incorporate an error detection and correction scheme approved by the network operators / stakeholders to ensure the data is transmitted and received accurately.

c) The network shall be capable of detecting and displaying certain conditions. These conditions shall be recorded in an error log that may be displayed or printed on demand, and shall archive the conditions for a minimum of ninety (90) days:

   i. Power reset or failure of any component of the network.

   ii. Communication loss between any component of the network.

   iii. Authentication failure. This may be either a logon failure or key exchange failure.

3.2 Firewalls

3.2.1 General Statement. A firewall is simply a group of components that collectively form a barrier between two networks. Implementation of suitable firewalls is strongly *recommended*. The following key requirements shall apply to a firewall:

a) Firewall technology shall be implemented at network edges to protect against unauthorized access of internal information assets.

b) All external and Demilitarized Zone (DMZ) traffic shall be routed through firewall devices. Network trafficking rules shall be applied in line with operational design.

c) Network trafficking rules shall include but not be limited to the following:

   i. Allow for stateful connection monitoring.

   ii. An incoming packet shall not have a source address of the internal network,

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

iii. An incoming packet shall not contain Internet Control Message Protocol (ICMP) traffic,

iv. An incoming packet shall have a publicly registered destination address associated with the internal network if using static or dynamic Network Address Translation (NAT),

v. An outgoing packet shall have a source address of the internal network,

vi. An outgoing packet shall not have a destination address of the internal network,

vii. An incoming or outgoing packet shall not have a source or destination address that is private or in a reserved space,

viii. Sources of traffic from Internet sites that are known to contain spam, offensive material, etc., should preferably be blocked.

ix. Any source routed packets or any packets with the Internet Protocol (IP) options field set shall be blocked.

x. Inbound or outbound traffic containing source or destination addresses of 127.0.0.1 or 0.0.0.0, link local (169.254.0.0 - 169.254.255.255), or directed broadcast addresses shall be blocked.

d) When required to allow services, such as voice (Voice over IP - VoIP), instant messaging, presence, mobility services, multimedia (Multimedia over IP - MoIP), etc., to securely traverse network borders and NAT functionality, firewall technologies shall include the following additional rules:

i. Use a Session Initiation Protocol (SIP) proxy server or H.323 gatekeeper outside the firewall, with the firewall configured to allow communication of endpoints only with the proxy server, or

ii. Be configured to function as application-layer gateways that monitor all SIP and H.323 traffic in order to open and close restricted ports as required and rewrite the IP addresses within the unencrypted application-layer messages, or

iii. Use a Session Border Controller (SBC), also known as an application router, to allow for end-to-end VoIP communications across multiple IP networks while allowing VoIP endpoints such as VoIP gateways, IP phones, and IP soft phones;

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

which are behind a Network Address Translation (NAT) firewall, to communicate with VoIP endpoints on external IP networks.

e) Internet Engineering Task Force (IETF) draft proposals for NAT traversal, such as Connection Oriented Media Transport, Middlebox Communications (Midcom), Simple Traversal of UDP through NAT (STUN), and Traversal Using Relay NAT (TURN), when taken singularly, do not provide a complete, comprehensive solution. IETF Internet Draft Interactive Connectivity Establishment (ICE) is a proposed methodology for NAT traversal for SIP. ICE makes use of existing protocols, such as STUN, TURN, and even Realm Specific IP (RSIP). ICE works through the cooperation of both endpoints in a session.

f) Remote management of firewall technologies shall be via encrypted communications or disallowed entirely.

g) Firewall policies shall be reviewed, tested, and audited, on a frequency determined and documented by the network operator / stakeholder.

3.2.2 ***Multiple Networks***. In the event a particular network server is utilized in conjunction with other networks, all communications, including remote access, shall pass through at least one approved application-level firewall and must not have a facility that allows for an alternate network path. If an alternate network path exists for redundancy purposes, it shall also pass through at least one application-level firewall.

3.2.3 ***Firewall Audit Logs***. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

a) all changes to configuration of the firewall;

b) all successful and unsuccessful connection attempts* through the firewall; the number of unsuccessful connection attempts shall be a configurable parameter by the network operator / stakeholder; and

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

c) the source and destination IP addresses and port numbers for ingress traffic; and
Note: In cases where a NAT firewall does not have the capability to log the destination IP address if found in its NAT Forward Table, logging of the destination IP address is not necessary.

d) MAC addresses for egress traffic. At a minimum, the initial successful connection with a new MAC address.

** Please note, a configurable parameter, 'unsuccessful connection attempts', may be utilized to deny further connection requests should the predefined threshold be exceeded. The network operators / stakeholders must also be notified.*

3.3 Password Protection and Logins

3.3.1 Device Passwords and Settings.

a) Device passwords shall be immediately changed before or upon device installation and shall conform to requirements set forth by the network security policy;

b) Networking devices shall be configured to retain their current configuration, security settings, passwords, etc., during a reset or reboot process;

c) All administrative passwords shall be changed regularly (recommended every 45 days), or minimally, any time IT staff leave the organization. Password aging is strongly *recommended*;

d) Only individual accounts that are uniquely tied to an individual shall be utilized – no shared or generic accounts shall be used except for those used for read-only access, as described elsewhere in this document;

e) Access for terminated or suspended employees shall be removed within 24 hours of notification;

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

f) Access for employees who have been transferred to other departments shall be removed in cases where that employee's new job function are no longer related to their previous access rights;

g) Thresholds shall be configurable to allow only a certain number of unsuccessful logon attempts via a given user's password. Once the threshold is exceeded, the account shall require administrative intervention to unlock*; and

**Please note that account lockouts can themselves be leveraged as a Denial of Service attack.*

NOTE: *GLI **recommends** the following minimum password criteria:*

1) 8 – 14 characters in length;
2) A combination of at least three of the following components:
   Uppercase letters
   Lowercase letters
   Numbers
   Special characters
3) Not part of the user's login name;
4) Not be part of the previous password (example last password was "Doggie79" new one shouldn't be "Doggie80"); and
5) Should avoid personal information of the user that someone could know about (i.e. birthday, kid's names, etc.).

It is important to note here that the above guidelines for passwords and settings are based upon recommendations provided by industry standards organizations such as NIST, ISO, and IEEE. While sufficiently complex passwords are effective in and of themselves, they can also be easily compromised by end-users. For example, if the passwords are difficult to remember, many end-users simply opt to write them down, thus undermining their benefit. This tradeoff should be considered when establishing any password regimen.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

3.3.2 ***Logins***. All network users shall have a unique identifier (user ID or login) for their specific use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

a) User IDs shall be capable of tracing activities to the responsible individual. Regular user activities shall not be performed from privileged accounts. In exceptional circumstances where there is a clear need, the use of a shared user ID for a group of users or a specific job function can be used. Generic IDs for use by an individual should only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g. read only access), or where there are other controls in place (e.g., password for a generic ID only issued to one staff at a time and logging such an isolated instance).

b) Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as smart cards, tokens, or biometric means, are strongly *recommended*.

3.4 Multi-layered Protection

3.4.1 ***General Statement***. Multi-layered protection shall be deployed wherever and whenever possible. Networks with different functions shall be implemented separately. For example, slot accounting and ticketing networks shall be kept separate and non-routable if possible. This approach keeps any successful intrusion isolated. Multiple security layers should be implemented to complement one another insofar as what one misses, the other catches.

3.5 Encryption – Transmission and Storage

3.5.1 ***Transmission Encryption Technologies***. All networks and security protocols shall deploy and support encryption suited to the communication method for the transmission of confidential or sensitive data/information. Note that what constitutes “confidential or sensitive data/information” can vary widely. At a minimum, highly personal information such as PINs

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

and Social Security Numbers would be viewed as confidential. The importance of other data may vary as a function of how critical that data is to the integrity of the network and/or the needs of the business. The network operator must assess the type of data items that the network carries and determine the relative sensitivity of this information. This assessment will then serve as a guide to the types of security measures that are appropriate for the network.

3.5.2 ***Additional Protection Methods***. Protection methods listed below shall also be considered and utilized as technically feasible for additional protection of the network:

a) IPSec– A suite of authentication and encryption protocols suitable for all types of Internet Protocol (IP) traffic that is used to create Virtual Private Networks (VPNs). IPSec allows confidential information to be sent securely between two end-stations or networks over an un-trusted communications medium. This shall be considered as a technology for securing Internet and other IP communications in connecting authorized external customers at defined locations;

b) Secure Shell (SSH) – Shall be deployed solely for the remote administration of confidential data/information and their systems;

c) Secure Sockets Layer (SSL) – The Secure Sockets Layer specification shall be deployed to provide secure access to confidential data/information on web servers. When SSL is used to protect confidential information, the most current version shall be used with 128-bit encryption;

d) Virtual Private Networks (VPNs) – Shall be deployed in environments where data-link-layer encryption is not a practical solution to maintain and operate. VPN technology using IPSec or SSL encryption can be implemented independently from a particular link-layer communications technology (e.g., High-Level Data Link Control/HDLC, Frame Relay, Fiber Distributed Data Interface/FDDI, Ethernet, Gigabit Ethernet, Asynchronous Transfer Mode/ATM, etc.) As such, this best practices resource strongly encourages the use of VPN technology to secure confidential communications;

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

e) Data-Link (symmetrical) Encryption – Shall be used in environments where Virtual Private Network management is not a reasonable encryption implementation to maintain and operate, or where the use and management of VPN technology is not warranted;

f) Secure /Multipurpose Internet Email Extension (S/MIME) – like Pretty Good Privacy (PGP), S/MIME is a standards-based security enhancement to secure email and message attachments that provides strong authentication through digital signatures, message confidentiality, integrity and non-repudiation.

g) Pretty Good Privacy (PGP) – Shall be used to protect sensitive information, transmitted via e-mail, using a minimum key-size of 2048 bits. Public key information may be maintained on public or internal PGP key servers.

h) Public Key Infrastructure (PKI) – Recommended PKI-based technical functionality is defined by Standard X.509 and its extensions, in the evolving definition developed by the Internet Engineering Task Force (IETF), through the PKIX Standards Development Task Group. This document provides and defines certified identification of digital signatures having integrity, non-repudiation, and authentication.

3.5.3 Disk {Storage} Encryption.

a) Anywhere sensitive information is stored on disk it shall utilize some form of encryption.

b) Databases that are used to store sensitive or protected information shall be configured to enable encryption by default. The encryption of sensitive database fields is also acceptable if another method is used to prevent network sniffing.

3.5.4 Storage Encryption Technologies. All confidential data/information residing on Direct Attached Storage (DAS) devices, Network Attached Storage (NAS) devices, Storage Area Network (SAN) devices, and all portable storage devices[3], shall be encrypted and shall employ at least one or more of the encryption methods listed below for the protection of confidential data and protected information:

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

a) Full-Disk Encryption – Encrypts all data on a hard drive for a client device. This includes the entire operating system, all applications, and all data/information. Full-disk encryption software contains components that are independent of the operating system and execute before the operating system is loaded as well as authentication. The system is rendered unintelligible and unusable in the event of a cyber crime or terrorism.

i. ***Full-Disk Encryption shall have the following capabilities:*** Pre-boot authentication for laptops/table PC's; file and folder-based encryption capabilities built into the operating system; supports single sign-on; remote install capability; supports multiple algorithms and has the ability to disable supported and unsupported algorithms in the event of conflict.

b) File (Folder) Encryption – Provides encryption for specific files or folders. File-encryption solutions provide automatic security since each new file/folder encryption capability must be manually turned off/on.

i. ***File (Folder) Encryption shall have the following capabilities:*** Must be able to support all state operating systems, all applications and related software programs in addition to productivity software for the state; ability to support a multitude of server(s) and file systems; provide simple recovery mechanisms for the recovery of lost keys of encrypted files/folders; integrate seamlessly with mobile email; supports security concepts and methods of "separation of duties".

c) Back-up and Archive Media Encryption – Provides benefits not only for protecting data in storage but also in the disposal of backup media. Many privacy regulations include disposal of back-up and archive media, while disclosure regulations generally dictate a retention period for back-up and archive data. Without encryption, media disposal is difficult; therefore, many entities keep back-up and archive media longer than needed or legally prudent. By deleting the encryption key, media is rendered unreadable. With a rotating key sequence, a regular pattern of retention and disposal can be automatically enforced.

i. ***Back-up and Archive Media Encryption shall have the following capabilities:*** Integrates seamlessly into the backup process and devices; offers flexible options

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

for data restoration and disaster recovery and supports various backup media types used by the state.

d) Mass Storage (SAN/NAS) Encryption – provides for encrypting large volumes of active data/information. Mass storage devices refer to a Storage Area Network (SAN) and Network-Attached Storage (NAS) data management solutions. Recently, the boundaries between NAS and SAN systems have overlapped with some products providing both file level protocols (NAS) and block level protocols (SAN).

i. ***Mass Storage (SAN/NAS) Encryption shall have the following capabilities:*** Supports encryption throughout the lifecycle of all data/information whether in storage or in transit; encryption and decryption methods must have both logical and physical segmentations; provide efficient encryption/decryption across multiple mass storage device types including fiber channel disks within an IP based network environment.

e) Database Encryption – Entails encrypting physical data within a database by encrypting the entire database, or calling functions, or stored procedures and database triggers, or natively using Database Management System (DBMS) encryption features to encrypt all or in part (column, row, or field level). Database encryption can be implemented at the application level.

i. ***Database Encryption shall have the following capabilities:*** Supports symmetric and asymmetrical encryption; ability to perform column/row level encryption vs. full database encryption for greater flexibility; supports multiple database platforms and operating systems; ability to encrypt and decrypt at the application and/or field level; supports separation of duties between the database administrator and the "key" administrator.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

f) Encryption for Removable Storage Drives and Devices – Provides encryption for smaller portable devices and existing datasets. A Universal Serial Bus (USB) flash drive comprises a memory card that plugs into a computer's USB port and functions as a portable hard-drive that does not contain moving parts. A USB flash drive is commonly known as a "flash drive," "thumb drive", "pen drive", "keychain drive", "key drive", "USB key", "USB stick", or "memory key".

i. ***Encryption for Removable Storage Drives and Devices shall have the following capabilities:*** USB flash drives must have password/security capabilities built into the device. USB flash drives and removable storage devices can be purchased with encryption software installed on the device hardware, or file-encryption software can be purchased after-the-fact for installation.

3.5.5 ***Encryption Keys Minimum Width***. The minimum width (size) for encryption keys shall be 128 bits for symmetric algorithms and 1024 bits for public keys.

3.5.6 ***Encryption Key Handling***. There must be a secure method implemented for changing the current encryption key set. It is not acceptable to only use the current key set to "encrypt" the next set. An example of an acceptable method of exchanging keys is the use of public key encryption techniques to transfer new key sets.

3.5.7 ***Encryption Key Storage***. There must be a secure method in place for the storage of any encryption keys. Encryption keys must not be stored without being encrypted themselves.

3.6 External Connections

3.6.1 ***General Statement***. External connections to operational networks shall be routed through secure gateways and protected by at least one of the following encryption methods, as applicable:

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

a) Transport Layer Security (TLS) or Secure Socket Layer (SSL) shall be employed between a web server and browser to authenticate the web server and, optionally, the user's browser. Implementations of TLS and SSL shall allow for client authentication support using the services provided by Certificate Authorities. The use of SSLv2 and TLSv1.0 are deprecated as of the publication date of this document.

b) IP Security (IPSec) shall be used to extend the IP communications protocol, providing end-to-end confidentiality for data packets traveling over the Internet. The appropriate mode of IPSec shall be used commensurate with the level of security required for the data being transmitted: sender authentication and integrity without confidentiality or sender authentication and integrity with confidentiality.

c) VPNs shall be used to interconnect two networks that traverse and communicate over insecure networks, such as the public Internet, by establishing a secure link, typically between firewalls, using an industry accepted cryptographic tunneling protocol such as IPSec or L2TP. VPNs are recommended for use in remote access.

d) Remote Authentication Dial-In User Service (RADIUS) is a client/ server software protocol that enables network access servers to communicate with a central server to authenticate and authorize remote users to access systems or services; strong authentication shall be used for dial-up modem systems.

e) Dial-up desktop workstation modems shall be disabled and removed. The use of hardware and inventory scanning tools to verify the presence and configuration of dial utilities and modems shall be implemented. Any use of dial-up modem systems shall adhere to policies accepted by the network operator / stakeholder which shall include:

   i. A complete, current list of all authorized personnel having modem access privileges.
   ii. Automatic disconnection after a specified period of inactivity. Inactivity parameters shall be determined by the network operator / stakeholder in line with operational needs.
   iii. The recommended use of security tokens.
   iv. Immediate termination of modem access privileges upon employment transfer, re-assignment, or termination.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

f) Where data sensitivity dictates, strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, and smart cards, shall be used once permission to connect has been granted.

g) External connections shall be removed promptly when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection.

3.7 Antivirus and Malware Protection Programs

3.7.1 ***Antivirus and Malware Protection***. Where applicable, antivirus and malware programs utilized for network security purposes shall:

a) Be mandatory on all systems.

b) Be updated automatically, or if not feasible or possible due to other constraints, be updated regularly through some manual means. If manual updates are required, their frequency shall be stated in the Security Policy.

c) Include both file system scanning and real-time processing. (Note that scans can adversely impact the performance of a live network, so this is a factor that should be considered when selecting a specific approach.)

d) Ideally leverage multiple vendor solutions between host systems and gateway services (e.g., email gateway). This is consistent with a multilayered implementation philosophy.

3.8 Software Updates and Patches

3.8.1 ***General Statement***. The network operators / stakeholders should develop and implement written procedures that outline roles and responsibilities for software updates and patch management that cover the following activities:

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

a) The network operators / stakeholders shall proactively monitor and address software vulnerabilities of all network devices (routers, firewalls, switches, servers, storage devices, etc.) by ensuring that applicable patches are acquired, tested, and installed in a timely manner.

b) Where possible, patches shall be installed and validated in a test environment prior to their introduction to a production environment. Testing will help to expose detrimental impacts to software applications and/or network devices prior to implementation in a live network.

c) Where possible, the installation of patches shall be completed with the use of automated tools such as Windows Server Update Services (WSUS) or local repositories (UNIX variants). The status of deployed patches shall be monitored.

d) Where possible, systems configurations shall be backed up prior to patch installation.

3.9 Disaster Recovery (Logical)

3.9.1 ***General Statement***. Networks are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) stemming from a variety of sources such as natural disasters, hackers, viruses, etc. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the network operator's / stakeholder's risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the network operator's / stakeholder's control (such as electric power or telecommunications), and the network operators / stakeholders may be unable to ensure their availability. Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. Disaster recovery is intended to ensure that all critical data is retrievable on-demand and that it can be brought back to a usable state as quickly and efficiently as possible.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

3.9.2 ***Disaster Recovery Planning***. Components of disaster recovery and contingency planning shall reflect the following criteria:

a) Ongoing business impact analysis should be completed in an effort to identify and prioritize critical IT systems and components.
b) Maintenance and preventative controls should be implemented to reduce the effects of system disruptions and increase system availability.
c) Thorough recovery strategies must be implemented to ensure that the systems may be recovered quickly and effectively following a disruption. These strategies must include proper management of backup, replications, and failover systems.
d) A contingency plan must be developed and adhered to and shall contain detailed guidance and procedures for restoring damaged systems and/or data.
e) Planned testing, training, and exercises of contingency plans must occur regularly in an effort to expose gaps in the effectiveness of the plan execution and to ensure that personnel are familiar with their execution.
f) Contingency plans must be living documents that are updated regularly to remain current with systems changes and enhancements.

3.10 Intrusion Detection and Prevention

3.10.1 ***General Statement***. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to thwart possible incidents.

3.10.2 An Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS) shall be integrated into operational networks to proactively monitor all network devices for unauthorized intrusion, and shall conform to the following minimum criteria:

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

a) Intrusion Detection Systems shall be implemented both internally and externally in addition to existing firewall solutions. Intrusion detection logs shall be reviewed regularly by the network operators / stakeholders and all incidents shall be reported and resolved in a timely manner.

b) In respect to servers, Intrusion Detection Systems shall monitor for unauthorized changes made to files (file integrity), especially critical system files.

c) Procedures shall be implemented that provide for the review of network traffic. Network traffic shall be reviewed for the presence of anomalies that may be indicative of attacks or incorrectly configured devices.

d) Intrusion Prevention Systems shall include user-defined security parameters that will help establish performance baselines useful in establishing an appropriate set of security policies.

e) Application Vulnerability Description Language (AVDL) is a proposed security interoperability standard. AVDL creates a uniform way of describing application security vulnerabilities using Extensible Markup Language (XML). The XML-based technology will allow communication between products that find, block, fix, and report application security holes. Use of AVDL is *recommended* but not required.

f) Intrusion prevention technologies can reduce the number of false alarms by focusing on real-time heuristic behavior rather than using signature-matching technology to identify a potential network attack. Intrusion prevention technologies can also prevent "zero-day" attacks, which exploit previously unknown weaknesses, because they respond to a change in the normal state of operation. However, false positives can still be common.

g) IPS systems shall be utilized on systems or devices that cannot be properly patched to provide the appropriate level of security for those systems. IPS devices shall also be utilized to protect systems with known vulnerabilities during the extended time required for the patch management process.

3.10.3 ***Intrusion Protection***. All servers shall have sufficient physical / logical intrusion protection against unauthorized access. Ideally, the system should require manufacturer and network operators' / stakeholders' authority, thus providing joint, but not separate, access.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

Whereas an IDS is capable of detecting and reporting an unauthorized intrusion, an IPS is designed to prevent unauthorized access and disallow that traffic from gaining access in the first place.

3.11 Vulnerability Scanning

3.11.1 ***General Statement***. Where practical, network and host vulnerability scanners shall be used to test for the vulnerabilities of internal network devices, applications, and network perimeter defenses, as well as adherence to security policy and standards.

3.11.2 ***Vulnerability Scanning Tools***. Where technically feasible, an automated vulnerability scanning tool shall be used to scan a network for known "vulnerable services" (e.g., a system that allows anonymous File Transfer Protocol (FTP), sendmail relaying, etc.). It should be noted, however, that some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the vulnerabilities flagged by the automated scanning software may actually be vulnerable for a particular site but may be configured that way because the particular network environment requires it.

3.11.3 ***Vulnerability Scanners***. It is *recommended* that vulnerability scanners have the ability to handle the following minimum tasks:

a) Inventory systems and services including applied patches.
b) Identify security holes by confirming vulnerabilities.
c) Provide comprehensive reports and charts for effective decision-making and improved security.
d) Define and enforce valid security policies when used during security device installation and certification.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

e) Use stealth scanning to verify proper operation of IDS/IPS appliances.

f) Ideally vulnerability scanning should include both network and application level scanning.

Any of the above may be replaced by a manual process when needed/desired. This may be especially desirable for item b) as automated tools to verify vulnerabilities can cause outages.

3.12 Logging

3.12.1 Security Logging.

a) Logging capabilities shall be enabled on devices where supported.

b) Logs should be reviewed, on a frequency determined and documented by the network operator / stakeholder. This includes manually verifying automated log analysis tools.

c) Logs shall be held locally and be periodically mirrored on a centralized server to prevent system-level tampering of the data.

d) All network devices shall leverage Network Time Protocol (NTP) servers to standardize time stamps for log data to ensure a proper timeline can be recreated in the event of an incident.

3.12.2 Clock Synchronization. To facilitate logging, the clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed upon and accurate time source.

3.13 Remote Access

3.13.1 General Statement. Remote access is defined as any access to the system outside of the 'trusted' network. Remote access, where permitted, shall authenticate all computer systems

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

based on the authorized settings of the network or firewall application that establishes a connection with the network. The security of remote access will be reviewed on a case-by-case basis, in conjunction with the current technology and approval from the network operator / stakeholder.

3.13.2 ***Remote Access Requirements.*** If supported, a network may utilize password-controlled remote access as long as the following requirements are met:

a) A remote access user activity log shall be maintained as described below;
b) No unauthorized remote user administration functionality shall be permitted (adding users, changing permissions, etc.);
c) No unauthorized access to a database other than information retrieval using existing functions shall be allowed;
d) A network filter (firewall) shall be installed to protect access.

NOTE: *GLI acknowledges that the system manufacturer may, as needed, remotely access the network and its associated components for the purpose of product and user support, if permitted.*

3.13.3 ***Remote Access Log Auditing.*** The network server must maintain an activity log either automatically or have the ability to manually enter the logs depicting all remote access information. Remote access logs shall minimally include the following:

a) Log-on name of the user;
b) Time and date the connection was made;
c) Duration of connection; and
d) Activity while logged in, including the specific areas accessed and changes that were made.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

CHAPTER 4

4.0 WIRELESS NETWORKS

4.1 Industry Standards

4.1.1 Industry Standards for Wireless Networks. The majority of wireless standards in use today evolved from the work of the Institute of Electrical and Electronics Engineers (IEEE). This body develops standards for a wide range of technologies including wireless. The IEEE developed the first wireless LAN standard, 802.11, back in 1997. Multiple iterations of this basic wireless standard have been promulgated since that time.

4.2 Unique Considerations

4.2.1 General Statement. The wireless interface defines the communication boundary between two entities, such as a piece of software, a hardware device, or the end-user. It may also provide a means of translation between entities, which do not speak the same language. This section deals with software interfaces which exist between separate hardware and software components that compose the wireless system, and which provide a programmatic mechanism such that these components can communicate.

4.2.2 Communication Protocol. Each component of a wireless network shall function as indicated by the communication protocol implemented. All communication between the server(s) and the mobile client shall use appropriate authentication and cryptographic protocols to provide mutual authentication of the mobile device and the server, ensuring the integrity of the data communicated, and for confidentiality, encrypting the data communicated. GLI strongly recommends the use of commercially available 802.1(x) protocol-compliant devices in conjunction with other applicable security conscience components. Any alternative

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

implementations will be reviewed on a case-by-case basis, with network operators / stakeholders approval.

4.2.3 ***Wireless Server Used with Other Systems.*** In the event the wireless server is utilized in conjunction with other systems; (i.e. On-Line Monitoring and Control Systems, Ticket Validation Systems, Progressive Systems, etc.) including remote access, all communications shall pass through at least one approved application-level firewall, and must not have a facility that allows for an alternate network path unless the alternate route conforms to the requirements of this document, and has independent security (i.e. the keys are not the same as other networks). One choice for network authentication is IEEE 802.1X. As an open standard with support for multiple authentication protocols, 802.1X is flexible enough to support everything from digital certificates to username/password authentication, and platforms from low-end PDA devices and mobile phones up to desktop and server operating systems.

NOTE: *Each wireless network reviewed by the independent test lab will be examined thoroughly to ensure that the proposed field configuration is secure. The independent test lab may provide additional security recommendations and provide on-site training to the network operator / stakeholder, if requested.*

4.2.4 ***Wireless Network Physical Security.*** A wireless network shall conform to the following minimum requirements:

a) Wireless Access Points (WAPs) shall be physically located such that they are not easily accessible to the general public;
b) If the above is not fesasible, all exposed Ethernet outlets shall be disabled to reduce the risk of network intrusion;
c) The wireless network should preferably be designed to be an independent (isolated) network in accordance with multiple layering techniques discussed earlier;

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

d) The network shall support monitoring for evidence of unauthorized entry. If entry has been detected, the network shall assert appropriate controls to lock down or disable the suspected entry point, if possible, and notify the network operator / stakeholder; and

e) The network shall retain evidence of any physical tampering of hardware components.

4.2.5 ***Wireless Network Software Security.*** A wireless network shall:

a) Be designed or programmed in such a way that it may only communicate with authorized wireless clients/devices. Software transferred between server and client/device must be implemented using a method that securely links the client/device to the server, such that the software may only be used by authorized clients/devices. In general, if certificates, keys, or seeds are used they must not be hard coded, and must change automatically, over time, as a function of the communication link. Each method shall be reviewed by the network operators / stakeholders and the independent test lab on a case-by-case basis;

b) Employ encryption and strong user authentication, with a recommendation of at least two methods of validation prior to opening a wireless session; Acceptable methods include : Username and password, a physical token, smart ID card, etc.;

c) Perform mutual authentication to ensure that clients only communicate with valid networks. One example of this type of authentication is the use of a digital certificate. Upon joining the network, the client/device is presented with a server-side digital certificate. If the client/device trusts the certificate, the authentication process continues. If the certificate is not trusted, the process terminates;

d) Validate clients/devices at pre-defined time intervals with at least one method of authentication as described above. This time interval shall be configurable based on network operators / stakeholders requirements;

e) Maintain a list (database) of authorized clients/devices, which it can communicate with. This list shall include the client/device name, a unique client/device ID and the corresponding hardware identifier (MAC); GLI recommends implementing MAC (Media Access Control) filtering to delay unauthorized users from gaining access to the wireless network;

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

f) Install and maintain a stand-alone stateful (i.e., based upon a state table) packet inspection firewall, which shall isolate the access points from other network components that the casino has deployed;

g) Obfuscate the Service Set Identifier (SSID) so that what networks it is connected to are not immediately apparent. Hiding the SSID only delays discovery.;

h) Close active sessions if user authentication has exceeded the number of failed attempts; the number of failed attempts shall be configurable based on network operators / stakeholders requirements;

i) Provide a printable report of failed network access attempts, including the time and date stamp, the device name, and the hardware identifier of all devices requesting access to the network; and

j) GLI r*ecommends* the use of strong user authentication, authorization and encryption, which will validate the user against a secure database. Communications between the network and the client device shall use protocols designed for securing, authenticating and encrypting wireless networks. One example of the appropriate protocol is IEEE 802.1x. It provides the framework required and permits the use of higher-level authentication methods such as those methods listed in the table below.

802.1x RECOMMENDED AUTHENTICATION METHODS		
AUTHENTICATION METHOD	ACRONYM	AUTHENTICATED AGAINST
Protected Extensible Authentication Protocol	PEAP	LDAP, RADIUS, Kerberos or Microsoft Active Directory servers, as well as local databases stored on the secure gateway controller.
Extensible Authentication Protocol- Transport Layer Security	EAP-TLS	
Extensible Authentication Protocol-Tunneled Transport Layer Security	EAP-TTLS	
Virtual Private Network with L2TP/IPsec	VPN	
Point to Point Tunneling Protocol	PPTP	
Secure Sockets Layer	SSL	

Table 1: Recommended authentication methods for use with 802.1x

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

k) Although, an intruder can monitor the communication link over the air, the data inside the encrypted tunnel is prevented from being intercepted by implementing one or more of the methods listed in the above table.

l) It is not recommended to use non-tunneled Extensible Authentication Protocol (EAP) methods listed below, because wireless data links could be compromised.

802.1X NON-RECOMMENDED AUTHENTICATION METHODS	
AUTHENTICATION METHOD	ACRONYM
Extensible Authentication Protocol	EAP
Extensible Authentication Protocol Message Digest 5	EAP-MD5
Lightweight Extensible Authentication Protocol	LEAP

Table 2: Non-recommended authentication methods for use with 802.1x

4.2.6 ***Component Failures.*** The wireless network shall have sufficient redundancy and modularity to accommodate a component failure to prevent the interruption of the wireless operations. In addition, there shall be redundant copies of each audit log and system database, where applicable, on the wireless server with open support for backups and restoration. This includes a wireless network that has support for failover redundancy. A backup scheme implementation must occur in compliance with the Disaster Recovery Policy, although all methods will be reviewed on a case-by-case basis by the independent test lab.

4.2.7 ***Recovery Requirements.*** In the event of a catastrophic failure when the wireless network cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following minimum information, as applicable:

a) Significant events;

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

b) Auditing information; and

c) Specific site information such as unique configuration settings, security accounts, etc.

4.2.8 Wireless Protocols and Communications. Where appropriate, the IEEE 802.11x standard shall be used with standard wireless networks: IEEE 802.11x (Wireless Local Area Network (WLAN)), IEEE 802.15 (Wireless Personal Area Network (WPAN)), and IEEE 802.16 (Wireless Metropolitan Area Network (WMAN)).

a) WLAN security is addressed in the transmission layer with the IEEE 802.11i draft standard and at the IP applications layer with standards and policy-based authentication and access control.

   i. The Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11 standard, should be considered compromised and unreliable;

   ii. The WiFi Protected Access (WPA2) standard and Protected Extensible Authentication Protocol (PEAP) with the IEEE 802.1x Network Port Authentication standard provides improved security.

   iii. WPA2 allows for automatically generated per-user, per-session keys through 802.1x. In addition, keys can be regenerated (re-keying) periodically to increase security.

   iv. Pre-Shared Key (WPA-PSK) is susceptible to "brute force attacks" (attacks predicated upon repetition). If it is used, strong passphrase use is also required. GLI r*ecommends* the use of a randomly generated passphrase longer than 16 characters containing all of the following:

      - Uppercase
      - Lowercase
      - Digits 0-9
      - Symbols.

   v. Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Therefore, it is important that the network operators / stakeholders assess risks more frequently

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

and test and evaluate system security controls when wireless technologies are deployed.

b) WLAN Wireless Access Point Device Security

i. The Service Set Identifier (SSID) shall be changed from the factory default setting and limit their identifying information.

ii. The broadcast SSID feature can be disabled, requiring wireless clients/devices to be pre-configured for a specific access point, and causing delays for unauthorized users.

iii. Management access passwords must be changed from their default setting and the cryptographic keys shall be changed from the factory default setting. Cryptographic keys shall be changed often.

iv. Access point devices shall be managed via network management tools using SNMPv3 or higher. If network management is not performed by the network operators / stakeholders, SNMP shall be disabled.

v. Access point devices that operate with a central controller are recommended and shall be disabled during off-hours, or when not in use.

vi. Access points that are connected to the Internet by any means must have their traffic use a Virtual LAN (VLAN) and/or Network Address Translation (NAT) . VLANs are covered by IEEE 802.1Q. The use of VPN shall be employed when accessing internal resources.

vii. Signal strength (signal-to-noise ratio) of Wireless Access Points shall be audited and reduced to encompass only desired areas.

viii. A list of authorized Wireless Access Points shall be maintained by the network operator. The network operator shall regularly scan for unauthorized access points broadcasting inside its defined network perimeter. These rogue access points can serve as an unprotected entry point into the network.

ix. A list of authorized Wireless Access Points shall be maintained by the network operator / stakeholder. The network operators / stakeholders shall regularly scan for unauthorized access points broadcasting inside its defined network perimeter.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

These rogue access points can serve as an unprotected entry point into the network.

c) Wireless Personal Area Network (WPAN) devices used for network access, internal network-based Internet access, and application software shall:

i. Be required to adhere to the same range of security requirements as WLAN client devices.

ii. Require PIN entry or other authentication.

iii. Invoke link encryption on all connections and broadcast transmissions.

iv. Be set to the lowest necessary sufficient power level as to keep transmission localized to the immediate area.

v. Require strong device passwords as to prevent the unauthorized use of said devices.

vi. Use application-level encryption, VPN technologies, and authentication.

vii. Be turned off when not in use.

d) Wireless Metropolitan Area Network (WMAN) connectivity used to interconnect buildings shall use VPN technologies and transmissions shall be encrypted.

e) Firewall technology shall be implemented at all wireless application gateways. This is an additional level of security that will reduce unauthorized access to operational networks.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

CHAPTER 5

5.0 SOCIAL ENGINEERING AND EDUCATION

5.1 General Statement

5.1.1 ***General Statement.*** Social engineering attacks include non-technical intrusions into a network using information acquired through human interaction and rely on tricks that prey on an individual being unfamiliar with emerging technology and protocols. The network operators / stakeholders should establish policies and implement the necessary training programs to care for these sorts of attacks.

5.2 Vendor Impersonations

a) Attackers place calls to internal employees impersonating hardware, software, or service vendors attempting to gather information pertaining to internal systems. Valuable information could include passwords or network device models.

b) Employees should be educated as to what could be considered sensitive information and to whom inquiries of this type should be directed to within the network operators / stakeholders.

5.3 Publicly Available Information

a) A review of publicly available information regarding operational networks shall be completed routinely. When possible, this type of information should be kept from public knowledge.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

b) Such information would include, but is not limited to: employee names, titles, phone numbers, and email addresses. Information such as this could prove useful to a network hacker.

5.4 Voicemail Security

a) With nothing more than a phone number, a hacker can access sensitive operational information that has been recorded on voicemails, in voicemail boxes with weak passwords.

b) A voicemail password policy regarding length and complexity shall be adopted and enforced by the network operator / stakeholder.

5.5 Targeted Email "Phishing"

a) Emails sent to individuals and groups within the network operators / stakeholders in order to attempt enticing the user to reveal sensitive information.

b) Spam firewall devices shall be integrated into the network operator / stakeholder's network to mitigate occurrences of "Phishing" emails being delivered to internal and external users.

c) Combination of standard Phishing attempts with Social Engineering techniques ("Spear Phishing").

d) Staff should be educated on how to recognize potential dangerous emails.

5.6 Sensitive Document Disposal

a) Documents containing sensitive information regarding network infrastructure should be disposed of when no longer needed.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

b) Paper documents and media such as CD or DVD should be shredded prior to leaving the establishment.

c) Hard drives and disk storage devices in computers and other electronic equipment such as photocopiers should be cleared of stored data at the end of their life cycle and prior to removal or disposal to prevent access to secure information. Any data archiving regulations and requirements must be observed.

Special Note: *Disposal and/or destruction of sensitive documentation and information may be regulated in a particular jurisdiction. Any such handling of sensitive documentation or information must comply fully with local regulatory practices. These practices should be documented in the Security Policy.*

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

CHAPTER 6

6.0 CLOUD COMPUTING RESOURCES

6.1 General Statement

6.1.1 This document will use the definition of cloud computing as published in NIST Special Publication 800-145:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

Additionally the terms Consumer(s), Client(s), and Provider(s) will follow the definitions from the same source.

6.2 General Considerations

6.2.1 ***Introduction.*** To varying extents, moving to a cloud solution from a more conventional client-server model results in a potential shift in the control of the operating environment. In most cases, this is intentional and considered to be part of the goal of outsourcing. The utilization of cloud computing resources can provide for increased computing resource availability enhanced monitoring of operations and enhanced back-up and recovery functions. While direct physical control of network resources is outsourced in a cloud computing environment, the use of discreetly located secure data centers latently provide a similar level of physical security than local data centers; albeit, in a slightly different way. in virtual cloud environments, security can be further enhanced by the ability to “roll” or transfer data easily to other data centers in the case of impending natural disasters or other potential failure scenarios.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

While the use of cloud computing resources can appear to offset at least some level of physical control it also potentially provides for enhanced overall security of the data by allowing the ability to be more agile with respect to overall monitoring, back-up, recovery and general system health activity.

6.2.2 ***Verification of authenticity.*** The identity of all parties cannot be taken at face value. An identity verification mechanism such as certificates must be employed and verified.

6.2.3 ***Service agreements****:* As portions of what would be local infrastructure are handled by a third party, the service level agreement should detail be detailed and able to comply with the established local Security Policy.

6.2.4 ***Physical Security.*** The Cloud provider must prove that their physical security is certified to a verifiable and auditable standard (e.g. ISO27001).

6.2.5 ***On-site Private Clouds***. On-site private clouds are cloud environments which are wholly located on the consumer's premises.

6.2.6 ***On-site Private Cloud Security.*** Security of the on-site private cloud is effectively the same as the recommendations set forth in the preceding sections of this document.

6.2.7 ***Off-site Private Cloud***. An Offsite private cloud may be secured in the same way as an on-site private cloud. No assumptions may be made about the level of protection given by the provider.

6.2.8 ***Public Cloud***. In a public cloud, as the ability to build a tunnel may not exist, all traffic to and from your application could be considered un-trusted sensitive data and will have to be encrypted by the application.

Copyright © 2013 Gaming Laboratories International, LLC All Rights Reserved.

APPENDIX

LIST OF FIGURES

Figure 1 – Sample Topology for a Wired Network

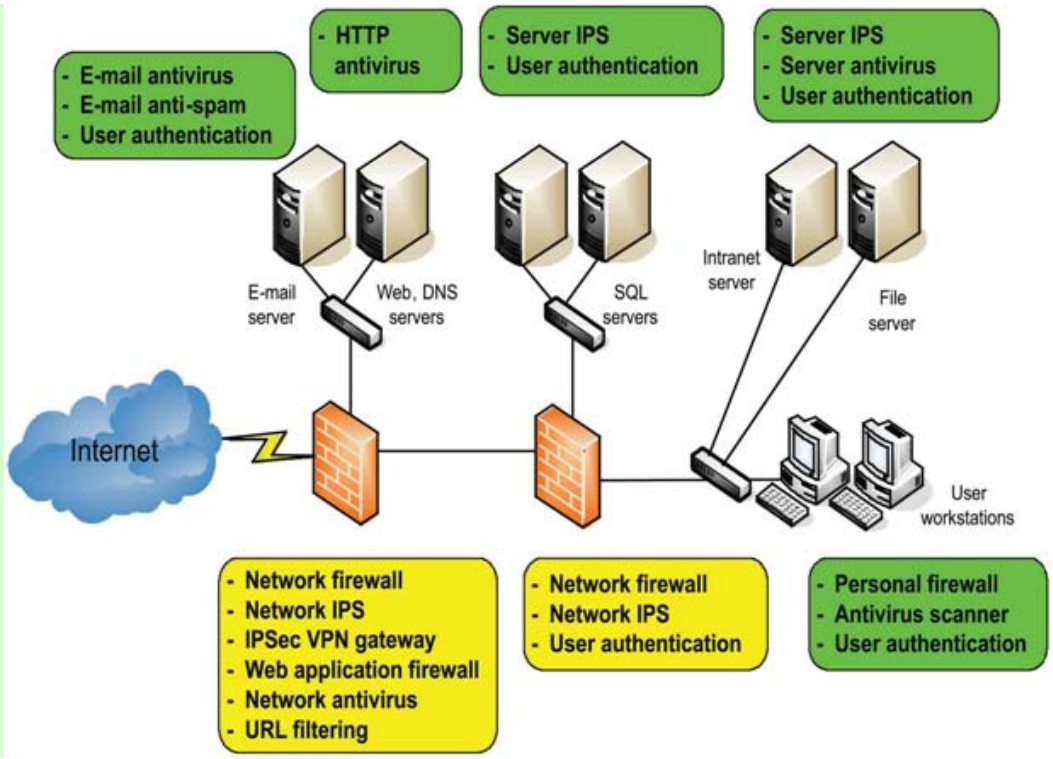
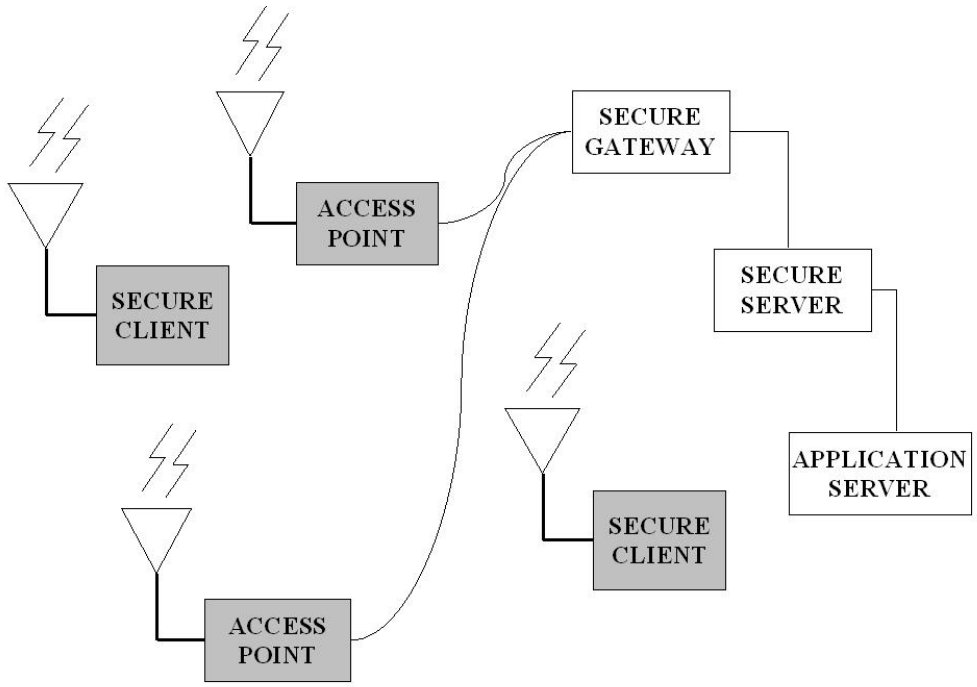


Figure 1 - Topology for a Wired Network, also showing possible security schema.

Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.

Figure 2 - Topology for a Wireless Network



Copyright © 2013 Gaming Laboratories International, LLC
All Rights Reserved.