GUIDELINE FOR BEST IT/CYBER POLICIES AND PROCEDURES

The purpose of this document is to provide guidance to licensed game operators with respect to setting and maintaining their cyber security policies and procedures. As you may know, gaming operations have become a frequent target of cyber-attacks at the international, national, and local level. The best defense against these attacks is setting and maintaining high levels of cyber security practices in your operation.

At present, the State of New Hampshire does not prescribe cybersecurity practices for licensed gaming operators. We are providing these best practices for educational purposes; however, we would anticipate that many if not all of these practices will become mandated through law or regulation at some point in the near future.

This guidance is separated into three distinct sections, Developing a Cybersecurity Plan, Implementing IT Procedures, and Accountability/Periodic Testing.

Developing A Cybersecurity Plan

All gaming operations should have a written cybersecurity plan that is specific to their gaming operation. The plan should be reviewed annually with management and updated as needed. An effective cybersecurity plan should:

- Conform to ISO 27001, or similar industry standards
- Designate a chief information security officer (CISO)
- Contain protocols for dealing with intrusions or security events including notice to the regulator of security breaches as soon as possible, in accordance with NH Rev Stat § 359-C:20
- Provide change management policies and documentation
- Articulate information sharing practices, specifically the administrative, technical, and physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customers' secure information

Implementing IT Procedures

In addition to the general procedures set out in the Cybersecurity Plan, gaming operations should have detailed procedures for protecting their IT infrastructure. These procedures should address the following topics:

I. *Intrusion Detection for local networks and Network Hardening*
   - Networks should be monitored in real-time
   - Networks should include endpoint detection and response (EDR)
   - Operators should consider 3rd party network monitoring when their IT staffs are not large enough to handle this task.

- Intrusion detection system/intrusion prevention systems should do all of the following:
    1. Listen to both internal and external communications
    2. Detect or prevent Distributed Denial of Service attacks
    3. Detect or prevent shellcode from traversing the network
    4. Detect or prevent Address Resolution Protocol spoofing
    5. Detect other Man-in-the-Middle indicators and server communication immediately.
- Operators should enable phishing reporting and email quarantines
- Operators should maintain Off-site Hot-site data mirroring and automated backup scheduling
- Operators should maintain a system event log that:
    1. Has automated or periodic manual reviews
    2. Has exception reports for certain activity
    3. Routinely audits Event Logs on all servers and privileged accounts for abnormalities
    4. Audits old software applications and hardware devices on network for sustainability and exploits (patch eligibility, end of life support)
- Operators should air gap PCs for standalone systems
- Operators should require domain connected PCs to auto restart to ensure updates installed

II. *User controls*

Operators should have written policies on access controls including requirements that:

- Ensure identities are proofed and bound to credentials
    1. Institute role-based access control
    2. Institute dual authentication
        - Multi-factor authentication (MFA) for all privileged accounts
    3. Maintain specific internal controls governing remote access to system
        - Limited to higher-level employees
    4. Establish controls for licensed employees of manufacturers
        - Require facility to take affirmative steps to allow such access, review, and audit on scheduled basis
- Require separation of departments
    1. Peer code review QA on in-house software development
    2. IT dept separate from all gaming departments
        - e.g. Departments unable to unilaterally provide credentials
- Local admin passwords change on regular basis (e.g. 90 days)
- Domain admin passwords change on regular basis (e.g. 90 days)
- Group Policy Objects (GPO) are set for password complexity
- Leverage Windows service accounts over user accounts to limit capabilities
- User access listings are reviewed quarterly

III. *Firewalls – production networks serving gaming systems are secured from outside traffic* Operators should periodically review firewall rules to ensure:
   - Blocking and disabling of unused ports
   - All network logs are audited for statistical analysis and reviewed to gauge unauthorized attempts and port exploitation on a 6mo cadence as part of change management policies
   - Firewall rules are created, audited and reviewed every 6 months
   - Separation of guest and gaming networks (VLAN)

Accountability/ Periodic Testing

The best policies and procedures are only effective if they are periodically reviewed and tested. Operators should:

I. Conduct an annual risk assessment, including at minimum:
   - Penetration test
   - Vulnerability assessment
   - Remediation or mitigation plans to address findings

II. Consider an annual independent entity review (e.g. SOC or ISO audit)

By implementing these practices and continuously updating and adapting the plan and policies, a licensed gaming operation can effectively mitigate the risk of cyber-attacks and protects it's assets, reputation, and players' trust.