

INFORMATION SECURITY POLICY



STRICTLY CONFIDENTIAL. ALL RIGHTS RESERVED.

The material contained within this document represents confidential and proprietary knowledge of WPT®Global. Any disclosure to third-party entities without the express written permission from WPT®Global is strictly prohibited. The unauthorized reproduction, storage, transmission, or any other form of dissemination of this document, whether by electronic, mechanical, photocopying, recording, or any other means, is explicitly disallowed without the prior consent of WPT®Global.

WPT®Global, all rights reserved.



Table of Contents

1. Introduction	4
1.1 Overview	4
1.2 Purpose	4
1.3 Scope	4
1.4 Policy Statement.....	5
2. Roles and Responsibilities.....	6
2.1 Information Security Manager.....	6
2.2 Employees	6
2.3 Contractors and Third-Parties.....	7
3. Risk Assessment	8
3.1 Risk Identification	8
3.2 Risk Evaluation	8
3.3 Risk Management	9
4. Data Protection.....	10
4.1 Data Classification.....	10
4.2 Data Access Control	10
4.3 Data Encryption	11
4.4 Data Backup and Recovery	11
5. Network Security.....	13
5.1 Firewalls	13
5.2 Intrusion Detection and Prevention	13
5.3 Secure Network Infrastructure	14
5.4 Virtual Private Network “VPN”	14
6. Application Security	15
6.1 Online Poker Application Security	15
6.2 Online Casino Application Security	15
6.3 User Authentication	16
6.4 Security Updates and Patch Management	16
7. Incident Response	17



7.1	Incident Detection	17
7.2	Incident Reporting	17
7.3	Incident Response Plan	17
7.4	Incident Recovery	18
8.	<i>User Training and Awareness</i>	<i>20</i>
8.1	Information Security Training	20
8.2	Phishing Awareness	20
8.3	Secure Usage of Online Gambling Platforms	21
9.	<i>Compliance</i>	<i>22</i>
9.1	Legal and Regulatory Requirements	22
9.2	Audit	22
9.3	Policy Compliance	23
10.	<i>Policy Review and Maintenance.....</i>	<i>24</i>
10.1	Review Period.....	24
10.2	Policy Updates	24
10.3	Exceptions	25
11.	<i>Definitions and Terms.....</i>	<i>26</i>



1. Introduction

1.1 Overview

This Information Security Policy “ISP” serves as a foundational guideline for WPT®Global, an online remote gambling operator that offers services including online Poker and online Casino games. It is crafted to align with our corporate mission and legal obligations while ensuring the secure operation of our digital platforms. Our commitment to information security is a crucial element of our business strategy, and this policy reflects that commitment.

1.2 Purpose

The purpose of this ISP is to:

- Define roles and responsibilities related to information security within WPT®Global.
- Outline security measures and procedures designed to protect company assets, customer data, and proprietary information.
- Foster a corporate culture that prioritizes security in all aspects of our business.
- Ensure compliance with relevant laws, regulations, and industry best practices.

1.3 Scope

This policy applies to all employees, contractors, third-parties, consultants, and other workers at WPT®Global, including all personnel affiliated with third parties. It covers all systems, networks, and data that support the provision of our services, as well as all physical locations where these resources are housed or accessed. This policy pertains to all forms of data — written, spoken, and electronic — handled by WPT®Global.



1.4 Policy Statement

WPT®Global commits to protecting the integrity, confidentiality, and availability of information by applying a risk management process, giving assurance to interested parties such as customers, stakeholders, and regulators. This includes:

- Implementing an effective information security management system that complies with international best practice standards.
- Regularly reviewing and updating our security measures in light of new technological developments and evolving threats.
- Conducting regular audits and risk assessments to ensure ongoing compliance with this policy.
- Ensuring all staff members are trained and aware of their responsibilities concerning data protection.

WPT®Global views breaches of this policy seriously. Violations will lead to disciplinary and/or legal action, where appropriate.



2. Roles and Responsibilities

2.1 Information Security Manager

The Information Security Manager “ISM” is a senior-level executive responsible for establishing and maintaining WPT®Global's security program to ensure information assets and technologies are adequately protected. Specific responsibilities of the ISMF include:

- **Developing Security Policies and Procedures:** The ISM oversees the development, implementation, and updates of this ISP to align with evolving business objectives and regulatory environments.
- **Risk Management:** The ISM coordinates the process of risk assessment, mitigation, and acceptance. This includes identifying potential security threats, recommending appropriate action, and making strategic decisions to manage risks.
- **Incident Response:** The ISM manages responses to information security incidents, ensuring they are properly reported, investigated, and resolved. The ISM will also oversee any subsequent analysis to learn from the incident.
- **Training and Awareness:** The ISM directs the development and delivery of an education program on information security and privacy matters for employees and other authorized users.

2.2 Employees

All employees at WPT®Global play a crucial role in maintaining information security. Employee responsibilities include:

- **Compliance with Policies:** Employees must read, understand, and follow the ISP. Any questions or concerns should be directed to the ISM or a supervisor.
- **Security Practices:** Employees must employ secure practices, such as:

Strictly-Confidential-WPT®Global

Information Security Policy



- maintaining strong unique passwords;
- locking computers when unattended; and
- only using secure networks for work-related activities.
- **Reporting Incidents:** Any suspected security incidents must be reported immediately to the ISM or a supervisor.

2.3 Contractors and Third-Parties

Contractors, consultants, and other third-party affiliates must also adhere to the ISP when handling WPT®Global information or accessing WPT®Global systems. Their responsibilities are the following:

1. **Understand and Comply with the ISP:** Before gaining access to any WPT®Global data or systems, third parties must confirm they have read and understood this ISP and agree to comply with it.
2. **Secure Practices:** Third parties should maintain secure environments when accessing WPT®Global data or systems. This includes using secure networks, protecting login credentials, and not sharing sensitive information without proper authorization.
3. **Reporting Incidents:** Like employees, third parties are responsible for reporting any suspected security incidents to the ISM or their WPT®Global contact immediately.

Each of these roles is integral to maintaining a secure environment at WPT®Global. Adherence to this policy is required, and failure to do so may result in consequences as outlined in the policy's enforcement provisions.



3. Risk Assessment

Risk assessment is a core component of our information security framework. This process is managed by the ISM and is crucial in identifying, evaluating, and managing potential risks that could impact the integrity, confidentiality, and availability of our data and systems.

3.1 Risk Identification

Risk identification involves identifying potential threats and vulnerabilities that could negatively impact WPT®Global's operations or assets. This is accomplished through a combination of:

- **Technical Assessments:** Regular vulnerability scans and penetration tests are conducted on our systems to identify potential technical weaknesses.
- **Third-Party Assessments:** We evaluate the security posture of third-party vendors who interact with our data and systems.
- **Staff Input:** Staff members are encouraged to report potential security concerns, like suspected phishing attempts or suspicious behavior.

3.2 Risk Evaluation

After potential risks are identified, they are evaluated based on their potential impact and the likelihood of their occurrence. Evaluation steps include:

- **Impact Assessment:** This assesses the potential harm that could be caused if a risk were to materialize, considering factors like financial loss, reputational damage, and regulatory penalties.
- **Likelihood Assessment:** This evaluates how likely it is for a risk to materialize, based on factors like the strength of existing controls and recent trends in threat activity.



- **Risk Rating:** Each risk is assigned a rating based on its impact and likelihood. This rating helps prioritize the risk for further management action.

3.3 Risk Management

Upon evaluation, risks are then managed in one of several ways:

- **Risk Mitigation:** This involves taking steps to reduce the impact or likelihood of a risk. For example, a risk of data breach could be mitigated by implementing stronger data encryption or user authentication controls.
- **Risk Transfer:** This involves passing the risk to another entity, such as through an insurance policy or a contractual agreement with a vendor.
- **Risk Acceptance:** If a risk is deemed acceptable given its potential impact and the cost of mitigation, it may be formally accepted. The decision to accept a risk should be informed by a careful cost-benefit analysis. This should be signed off by senior management.
- **Risk Avoidance:** If a risk is too high and cannot be adequately controlled, the activity causing the risk can be discontinued.

The results of risk identification, evaluation, and management processes are documented and reviewed regularly to account for changes in our operations or the threat landscape. The ISM oversees this process and collaborates with other departments to ensure that the risk assessment process aligns with business objectives and regulatory requirements.



4. Data Protection

Data protection is a critical component of our operations at WPT®Global. To ensure the security, confidentiality, and integrity of our data, we implement the following processes:

4.1 Data Classification

All data within WPT®Global is categorized based on its sensitivity and business impact. The categories include:

- **Public:** Information that can be freely disclosed to the public, such as marketing content or publicly available financial reports.
- **Internal:** Information used for internal purposes that would not harm WPT®Global if disclosed but should not be freely disseminated, such as internal policies or meeting minutes.
- **Confidential:** Sensitive information that could harm WPT®Global or its stakeholders if disclosed, such as proprietary business information, employee records, or strategic plans.
- **Restricted:** Highly sensitive information that could have severe negative impact if disclosed, such as credit card data, personal customer information, or cryptographic keys.

Each data category has corresponding security controls, and all employees are trained on how to handle data according to its classification.

4.2 Data Access Control

WPT®Global implements a role-based access control “RBAC” system to manage who has access to our data:



- **Roles and Permissions:** Employees are assigned roles based on their job responsibilities. Each role has specific permissions that determine what data they can access and what actions they can perform.
- **Access Requests:** Any request for access beyond an employee's role must be formally requested, justified, and approved by the appropriate manager.
- **Regular Audits:** Access logs are regularly reviewed and audited to detect and respond to any unauthorized access attempts or suspicious activity.

4.3 Data Encryption

Sensitive data, both at rest and in transit, is encrypted using industry standard cryptographic techniques:

- **Data at Rest:** All sensitive data stored on WPT®Global systems is encrypted using algorithms such as AES-256.
- **Data in Transit:** All sensitive data transmitted over networks is encrypted using secure protocols such as HTTPS, SSH, or TLS.

4.4 Data Backup and Recovery

Regular backups are crucial to recovering data in the event of a system failure or data loss event:

- **Regular Backups:** All critical data is backed up regularly to secure, encrypted storage.
- **Offsite Storage:** Backups are stored offsite to protect against physical threats to our primary data center.
- **Backup Testing:** The ability to restore data from backups is tested regularly to ensure our backup system is working properly.



The ISM oversees data protection efforts and ensures these processes align with our risk management strategy and regulatory requirements. Employees are trained on their responsibilities related to data protection, and failure to adhere to our data protection protocols can result in disciplinary action.



5. Network Security

At WPT®Global, we ensure our network security with the following processes and technologies:

5.1 Firewalls

Firewalls are our first line of defense against external threats. They are configured to control both inbound and outbound traffic, blocking unauthorized access while allowing legitimate traffic.

- **Perimeter Firewalls:** Installed at the edge of WPT®Global's network to monitor and control all incoming and outgoing traffic.
- **Internal Firewalls:** Used to segment our internal networks and protect sensitive areas from potential threats within WPT®Global.
- **Firewall Rules:** Regularly updated to reflect changes in our network configuration and threat landscape.

5.2 Intrusion Detection and Prevention

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are used to identify and block suspicious activity that could indicate a network attack.

- **Intrusion Detection Systems (IDS):** Monitors network traffic for signs of potential incidents, violations, or imminent threats, and alerts security administrators.
- **Intrusion Prevention Systems (IPS):** Identifies and mitigates attacks by automatically blocking malicious traffic and potentially harmful activities.
- **Regular Updates:** IDS/IPS signatures are updated regularly to ensure they can detect the latest threats.



5.3 Secure Network Infrastructure

The network infrastructure at WPT®Global is designed with security in mind:

- **Network Segmentation:** The internal network is divided into segments to contain potential security incidents and protect sensitive areas.
- **Least Privilege Principle:** Systems and users can only access the resources and perform the tasks necessary for their legitimate purposes.
- **Regular Audits:** Network configurations are regularly audited to detect vulnerabilities, ensure compliance with security policies, and verify the correct functioning of security controls.

5.4 Virtual Private Network “VPN”

All remote connections to WPT®Global’s internal network are made via a secure Virtual Private Network (VPN):

- **Secure Remote Access:** A VPN provides a secure tunnel between the user's device and WPT®Global’s network, ensuring that data is encrypted and secure from potential eavesdroppers.
- **Two-Factor Authentication:** All VPN users must authenticate themselves using two factors (something they know, like a password, and something they have, like a token or an app on their phone) to further increase security.
- **VPN Usage Policy:** Employees are trained on appropriate usage and the importance of always using the VPN for remote access.

All these processes and systems are overseen by the Information Security Manager and the IT department. Together, they ensure that our network security measures align with industry best practices and are effective against the latest threats.



6. Application Security

WPT®Global provides online services such as Poker and Casino games, and the security of these applications is of utmost importance. We ensure application security through the following measures:

6.1 Online Poker Application Security

The Online Poker application handles sensitive user information and transactions, requiring robust security measures:

- **Secure Software Development Lifecycle (SDLC):** Our Online Poker application is developed following a secure SDLC, which incorporates security at every phase, from initial design to development, testing, deployment, and maintenance.
- **Penetration Testing:** Regular penetration testing is conducted to identify potential vulnerabilities in the application.
- **Transaction Security:** Financial transactions within the application use secure cryptographic methods and protocols to protect against fraud and unauthorized access.

6.2 Online Casino Application Security

The Online Casino application also requires stringent security measures:

- **Secure SDLC:** Similar to the Online Poker application, the Online Casino application follows a secure SDLC.
- **Random Number Generation Security:** The integrity of our games depends on secure and fair random number generation. We use industry-standard algorithms and perform regular audits to ensure this critical system cannot be manipulated.
- **Transaction Security:** Financial transactions within the application are secured using robust cryptographic techniques.

Strictly-Confidential-WPT®Global

Information Security Policy



6.3 User Authentication

User authentication ensures that only authorized users can access their accounts:

- **Strong Password Policies:** We enforce strong password policies, requiring a combination of uppercase and lowercase letters, numbers, and special characters.
- **Two-Factor Authentication (2FA):** Users are required to provide two forms of authentication before gaining access to their account. This might be a combination of something they know (a password), something they have (a phone to receive an SMS code), or something they are (a fingerprint).
- **Account Lockout Policies:** To prevent brute force attacks, accounts are temporarily locked out after a certain number of failed login attempts.

6.4 Security Updates and Patch Management

Keeping applications up-to-date is critical for maintaining security:

- **Regular Updates:** Our applications are regularly updated to incorporate the latest security patches and mitigate identified vulnerabilities.
- **Patch Management Process:** Patches are tested in a controlled environment before being rolled out across the live applications. Any issues are addressed promptly to prevent disruptions to service.
- **Automated Update Checks:** Systems are configured to regularly check for and install updates, ensuring all applications remain up-to-date.

These application security procedures are overseen by the Information Security Manager and the development team. They ensure that our applications maintain the highest security standards, protecting both our users and our company.



7. Incident Response

Incident response is a crucial aspect of WPT®Global's overall information security strategy. It outlines how we identify, respond to, and recover from security incidents.

7.1 Incident Detection

Detecting a security incident as soon as possible is essential for limiting damage. We use the following methods for incident detection:

- **Monitoring Tools:** We use various monitoring tools that alert us to potential security incidents. This includes intrusion detection systems, log monitoring tools, and network traffic analyzers.
- **User Reports:** Staff members are trained to recognize signs of a security incident and to report it immediately. This can be an unusual system behavior, suspicious emails, or unexpected application behavior.
- **Regular Audits:** Regular audits of our systems help detect any irregularities that might indicate a security incident.

7.2 Incident Reporting

All suspected or confirmed security incidents should be immediately reported:

- **Internal Reporting:** Employees should report potential security incidents to their manager or directly to the Information Security Manager.
- **External Reporting:** In case of incidents involving customer data or critical system breaches, regulatory bodies and affected customers may need to be informed in compliance with relevant laws and regulations.

7.3 Incident Response Plan

When a security incident is identified, we follow a pre-defined incident response plan:

Strictly-Confidential-WPT®Global

Information Security Policy



- **Preparation:** We have an Incident Response Team “IRT” consisting of members from IT, HR, legal, and public relations. The team is trained and ready to respond to an incident at any time.
- **Identification:** The IRT first confirms whether an incident has occurred and assesses its scope and potential impact.
- **Containment:** Immediate action is taken to limit the impact of the incident. This might involve disconnecting affected systems from the network or blocking specific network traffic.
- **Eradication:** The source of the incident is identified and removed. For example, malware would be removed from systems, or unauthorized users would be blocked.
- **Recovery:** Systems are restored to normal operation. This might involve restoring systems from backups, reinstalling software, or changing passwords.

7.4 Incident Recovery

After an incident has been handled, the recovery phase ensures systems return to normal and lessons are learned:

- **System Restoration:** Systems affected by the incident are restored to normal operation, ensuring all traces of the incident are removed and security is reestablished.
- **Post-Incident Review:** A thorough review of the incident and the effectiveness of the response is conducted. This helps identify areas for improvement and update the incident response plan as necessary.
- **Reporting:** A formal incident report is prepared, detailing the incident, its impact, the response, and any lessons learned. This report may be necessary for insurance claims, regulatory compliance, or improving future incident responses.



The Information Security Manager is responsible for overseeing the incident response process, ensuring its effectiveness, and continually improving it based on lessons learned from past incidents.



8. User Training and Awareness

A critical aspect of information security at WPT®Global is user training and awareness. We implement the following programs to ensure that our employees and users understand their roles in maintaining security:

8.1 Information Security Training

All employees receive regular information security training:

- **Initial Training:** Upon hiring, employees undergo an orientation session that covers our Information Security Policy, including roles and responsibilities, data classification and handling, incident reporting, and secure computing practices.
- **Ongoing Training:** We provide regular training sessions throughout the year to keep employees up-to-date on the latest threats and best practices for security.
- **Specialized Training:** Employees with specific roles, such as system administrators or developers, receive additional training relevant to their duties.

8.2 Phishing Awareness

Phishing is a significant threat, and we ensure our employees can recognize and respond to it:

- **Phishing Training:** Employees are trained to recognize phishing emails and other types of social engineering attacks.
- **Simulated Phishing Campaigns:** We periodically send simulated phishing emails to test employee awareness and provide immediate feedback and training if an employee falls for the test.
- **Reporting Mechanism:** Employees are instructed to report suspected phishing attempts to the Information Security Manager or IT department.



8.3 Secure Usage of Online Gambling Platforms

Our users are crucial partners in security, and we provide guidance on how to use our platforms securely:

- **User Guides:** Our online platforms provide user guides that detail how to use the platform securely, such as setting a strong password and recognizing potential scams.
- **Notifications:** When significant security updates occur, we notify users and provide them with any necessary instructions or recommendations.
- **Customer Support:** Our customer support team is trained to answer security-related questions and provide users with guidance on secure use of our platform.

The Information Security Manager coordinates the training and awareness program, ensuring that content is updated regularly and that all employees receive the necessary training. By fostering a culture of security awareness, we can greatly enhance our overall information security posture.



9. Compliance

At WPT®Global, we are committed to maintaining full compliance with all applicable laws, regulations, and internal policies. Here's how we accomplish this:

9.1 Legal and Regulatory Requirements

Staying compliant with legal and regulatory requirements is crucial:

- **Identifying Requirements:** The first step is identifying all applicable legal and regulatory requirements related to information security. This includes privacy laws, data protection regulations, and specific requirements for the online gambling industry.
- **Implementing Controls:** Necessary controls are implemented to ensure compliance with these requirements. This may include technical controls (like encryption for data protection) and procedural controls (like consent mechanisms for data collection).
- **Regular Review:** The legal landscape frequently changes, so we regularly review our compliance with these requirements, adjusting our controls as necessary.

9.2 Audit

Regular audits ensure we maintain compliance with our policies and any external requirements:

- **Internal Audits:** We conduct regular internal audits of our information security practices to ensure compliance with this policy.
- **External Audits:** Independent auditors periodically review our information security posture. This could be a requirement of a regulatory body, or a voluntary review to ensure best practices are being followed.



- **Remediation:** Any issues found during audits are promptly addressed, and controls are improved to prevent similar issues in the future.

9.3 Policy Compliance

Ensuring compliance with our internal Information Security Policy is also critical:

- **Employee Acknowledgment:** All employees are required to read and acknowledge this policy. They understand that compliance with this policy is a condition of their employment.
- **Regular Training:** As part of our ongoing security training (see section 8), employees are reminded of their responsibilities under this policy and trained on any updates to the policy.
- **Policy Review:** The policy is regularly reviewed and updated to reflect changes in our environment and threat landscape. All changes are communicated to employees, and additional training is provided as necessary.

The Information Security Manager is responsible for ensuring WPT®Global's compliance with legal and regulatory requirements, coordinating audits, and enforcing compliance with this policy. Non-compliance is considered a serious matter and can result in disciplinary action, up to and including termination.



10. Policy Review and Maintenance

Regular review and maintenance of the Information Security Policy is essential to ensure it remains relevant and effective in the face of changing business needs, technological advances, and evolving threats.

10.1 Review Period

The Information Security Policy is reviewed on a routine basis:

- **Regular Reviews:** The Information Security Policy is reviewed at least annually by the Information Security Manager and relevant stakeholders.
- **Triggered Reviews:** Additional reviews may be triggered by significant changes, such as a new business process, introduction of new technology, significant security incident, or changes in legal or regulatory requirements.

10.2 Policy Updates

Updates to the policy are made as required:

1. **Change Proposal:** Any member of WPT®Global can propose changes to the policy. These proposals are reviewed by the Information Security Manager and relevant stakeholders.
2. **Change Approval:** Changes to the policy must be approved by senior management. Once approved, changes are implemented in the policy document and communicated to all affected parties.
3. **Change Communication:** All employees are informed of changes to the policy through email notifications and training sessions. They are required to read and acknowledge the updated policy.



10.3 Exceptions

Any exceptions to the policy must be handled with care:

- **Exception Request:** If an employee believes an exception to the policy is necessary, they must submit a formal request to the Information Security Manager detailing the proposed exception and justification.
- **Exception Review:** The Information Security Manager reviews the request, considering the potential risks and benefits. Additional stakeholders may be consulted.
- **Exception Approval:** If the exception is approved, it is documented and added to the policy until the next review. If not approved, the employee must comply with the existing policy.

The Information Security Manager is responsible for coordinating the review and maintenance of the Information Security Policy, ensuring that it continues to support WPT®Global's objectives and legal and regulatory requirements. The policy's effectiveness and compliance are periodically audited to ensure the highest standards of information security.



11. Definitions and Terms

- **Access Control:** A security technique that regulates who or what can view, use, or control resources in a computing environment.
- **Audit:** An official inspection of an organization's accounts or systems, typically by an independent body.
- **Backup:** A secondary copy of data, created for the purpose of restoring the data in case of loss.
- **Confidential Information:** Information that is not public knowledge and that is viewed as the property of the holder.
- **Contractor:** An external individual or organization that provides a specified service to the company, based on agreed terms.
- **Data Access Control:** Procedures and mechanisms in place to restrict access to sensitive data and information to authorized users only.
- **Data Backup and Recovery:** Processes involved in copying and archiving data to enable recovery in case of data loss or system failure.
- **Data Classification:** The process of organizing data into categories for its most effective and efficient use.
- **Data Encryption:** The process of converting plaintext into encoded data (ciphertext) to prevent unauthorized access.
- **Employees:** Individuals who are part of the organization and contribute to its functioning and productivity.
- **Exceptions:** Instances where a policy or rule may not apply or where deviation from the policy is allowed under specific circumstances
- **Firewall:** A network security system designed to prevent unauthorized access to or from a private network.
- **Incident:** A security event that compromises the integrity, confidentiality, or availability of an information asset.



- **Incident Detection:** The process of discovering or identifying a security incident or breach.
- **Incident Recovery:** The process of restoring affected services, data, and systems to their state before the security incident.
- **Incident Reporting:** The procedure for communicating information about a security incident immediately after it has been identified.
- **Incident Response Plan:** A set of instructions designed to help respond to and manage security incidents or cyber threats.
- **Information Security:** The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- **Information Security Policy:** A set of policies issued by an organization to ensure that all information technology users within the organization's domain abide by its rules and guidelines related to security.
- **Information Security Manager:** The individual within an organization who is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure that the company's information assets and technologies are adequately protected.
- **Information Security Training:** A program designed to educate employees about the dangers and threats they may face in the digital world and how they can protect the organization's information assets.
- **Intrusion Detection System "IDS":** A system that monitors network traffic for suspicious activity and alerts when such activity is discovered.
- **Intrusion Prevention System "IPS":** A system that inspects network traffic and can block or prevent suspicious activities.
- **Legal and Regulatory Requirements:** Obligations imposed on organizations by laws or regulatory bodies, particularly relating to information security and data privacy.



- **Online Gambling Platforms:** Digital platforms, like websites or applications, where users can engage in gambling activities.
- **Online Poker Application Security:** Security measures designed to protect online poker applications from cyber threats.
- **Online Casino Application Security:** Security measures aimed at safeguarding online casino applications against cyber threats.
- **Patch Management:** A strategy for managing updates and changes to software applications, including testing, scheduling, and applying patches in a timely and systematic manner.
- **Phishing:** A type of cyber-attack that uses email or a malicious website to infect a user's computer with malware or collect sensitive information.
- **Policy Updates:** Changes or amendments to a policy based on review findings, feedback, changing business requirements, or regulatory changes.
- **Review Period:** A predetermined timeline for evaluating or revising an existing policy or procedure.
- **Risk Assessment:** The overall process or method used to identify risks and vulnerabilities, assess the potential impacts, and determine appropriate responses.
- **Risk Evaluation:** The process of comparing the identified risk against predetermined risk criteria to determine the significance of the risk.
- **Risk Identification:** The process of finding, recognizing, and describing risks that could affect the achievement of an organization's objectives.
- **Risk Management:** The process of identifying, assessing, and controlling risks arising from operational factors and making decisions to mitigate those risks.
- **Secure Network Infrastructure:** A system designed to protect the integrity of the network and the data being transmitted over it.
- **Secure Usage of Online Gambling Platforms:** Guidelines and best practices for safely accessing and using online gambling platforms to prevent security breaches or cyber-attacks.



- **Security Updates:** Software patches or modifications intended to secure a system or fix vulnerabilities.
- **Social Engineering Techniques:** used by cybercriminals designed to deceive users into revealing sensitive information, like passwords or credit card numbers.
- **Third-Party:** An individual or organization that is indirectly connected to the organization, often through a contract or business deal.
- **User Authentication:** The process of verifying a user's identity before granting them access to specific data or systems.
- **VPN "Virtual Private Network":** A technology that allows secure and private internet access by creating an encrypted connection over a less secure network, typically the internet.