Web Filtering Policy

ISO 27001:2022

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	**Ayaz Sabir**
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

1. Executive Summary

The organization recognizes that internet access is essential for business operations while simultaneously presenting significant security risks that must be carefully managed. This Web Filtering Policy establishes a comprehensive framework for implementing, managing, and monitoring web filtering controls that protect organizational assets while enabling productive business activities. The policy aligns with ISO/IEC 27001:2022 security controls and supports the organization's commitment to information security excellence.

Web filtering serves as a critical component of the organization's defense-in-depth security strategy, providing protection against malicious websites, inappropriate content, and productivity-impacting activities. The implementation of these controls demonstrates the organization's commitment to maintaining a secure and productive work environment while ensuring compliance with applicable legal and regulatory requirements.

This policy applies to all organizational networks, systems, and personnel, establishing clear expectations for internet usage while providing the necessary flexibility to support legitimate business activities. The framework balances security requirements with operational needs, ensuring that web filtering controls enhance rather than hinder business productivity.

---

2. Policy Statement and Objectives

2.1 Policy Statement

The organization implements comprehensive web filtering controls across all network infrastructure to protect against web-based security threats, ensure appropriate use of internet resources, and maintain compliance with organizational policies and regulatory requirements. All internet access through organizational networks is subject to web filtering controls, monitoring, and logging in accordance with this policy and applicable legal frameworks.

The organization is committed to maintaining a balance between security protection and business productivity, ensuring that web filtering controls are implemented in a manner that supports legitimate business activities while preventing access to malicious, inappropriate, or non-business-related content. This approach recognizes that internet access is essential for modern business operations while acknowledging the inherent security risks that must be managed effectively.

2.2 Strategic Objectives

The primary objective of this web filtering policy is to establish a robust security posture that protects organizational information assets from web-based threats while enabling productive business operations. This includes preventing access to malicious websites that could compromise organizational systems, blocking inappropriate content that could create legal or regulatory risks, and managing bandwidth utilization to ensure optimal network performance.

The policy aims to create a secure and productive work environment by implementing controls that are transparent to users while providing comprehensive protection against emerging threats. The framework supports the organization's risk management strategy by reducing exposure to web-based attacks, data breaches, and compliance violations while maintaining the flexibility necessary to adapt to changing business requirements.

Additionally, the policy establishes clear accountability and monitoring mechanisms that enable the organization to demonstrate compliance with regulatory requirements, investigate security incidents, and continuously improve the effectiveness of web filtering controls based on evolving threat landscapes and business needs.

---

3. Scope and Applicability

3.1 Organizational Scope

This policy applies comprehensively across all organizational entities, subsidiaries, and business units, encompassing all network infrastructure, internet connections, and web-enabled devices. The scope includes traditional office environments, remote work locations, mobile devices, and cloud-based services that access the internet through organizational networks or security controls.

The policy extends to all personnel categories including full-time employees, part-time staff, contractors, consultants, temporary workers, and visitors who access organizational network resources. This comprehensive coverage ensures consistent application of security controls regardless of employment status or location, maintaining the integrity of the organization's security posture across all access points.

The framework encompasses all types of internet access including direct connections, wireless networks, virtual private networks, and cloud-based internet gateways. This broad applicability ensures that security controls remain effective as the organization adopts new technologies and work arrangements, providing consistent protection across evolving network architectures.

3.2 Technical Scope

The technical scope of this policy includes all network devices, security appliances, and software systems involved in providing, controlling, or monitoring internet access. This encompasses web filtering appliances, proxy servers, DNS servers, firewalls, and endpoint security solutions that contribute to the overall web filtering architecture.

The policy applies to all protocols and services used for internet communication, including HTTP, HTTPS, FTP, and emerging protocols that may be used to access web-based content or services. This comprehensive coverage ensures that security controls remain effective as communication technologies evolve and new methods of accessing internet content are developed.

Cloud-based services and software-as-a-service applications that are accessed through web browsers or web-based interfaces fall within the scope of this policy, ensuring that organizational data and systems remain protected regardless of where services are hosted or how they are accessed by users.

---

4. Regulatory and Standards Compliance

4.1 ISO 27001:2022 Alignment

This policy directly supports compliance with ISO/IEC 27001:2022 Annex A Control 8.23 regarding web filtering, which requires organizations to implement appropriate controls to manage access to web-based content and services. The policy framework ensures that web filtering controls are implemented systematically and maintained effectively to protect against web-based threats and inappropriate content.

The policy also aligns with Control 8.20 concerning network security management, ensuring that web filtering is integrated into the broader network security architecture and managed as part of comprehensive network protection strategies. This integration provides layered security that enhances the overall effectiveness of organizational security controls.

Additionally, the policy supports Control 5.10 regarding acceptable use of information and associated assets, establishing clear guidelines for appropriate internet usage while providing enforcement mechanisms that ensure compliance with organizational expectations and regulatory requirements.

4.2 Regulatory Compliance Framework

The organization recognizes that web filtering controls must comply with various regulatory requirements including data protection laws, employment regulations, and industry-specific security standards. The policy framework incorporates privacy considerations to ensure that monitoring and filtering activities comply with applicable privacy laws while maintaining the necessary level of security protection.

Employment law considerations are integrated into the policy to ensure that internet monitoring and filtering activities are conducted in accordance with applicable workplace regulations and employee rights. This includes providing appropriate notice to employees regarding monitoring activities and ensuring that disciplinary actions for policy violations follow established employment law requirements.

Industry-specific regulations that may impact web filtering requirements are addressed through the policy's flexible framework, which allows for additional controls or restrictions to be implemented as necessary to meet sector-specific compliance obligations while maintaining consistency with the overall organizational security strategy.

5. Web Filtering Architecture and Technology

5.1 Technology Framework

The organization implements a multi-layered web filtering architecture that combines various technologies to provide comprehensive protection against web-based threats while maintaining optimal network performance. This architecture includes proxy-based filtering systems that provide deep content inspection and analysis, DNS-based filtering that blocks access to malicious domains at the network level, and cloud-based security services that leverage global threat intelligence.

Proxy-based filtering serves as the primary mechanism for content inspection and control, providing the ability to analyze web traffic in real-time and apply granular filtering policies based on content categories, user groups, and business requirements. These systems include SSL/TLS inspection capabilities that enable the analysis of encrypted traffic while maintaining appropriate privacy protections for sensitive communications.

DNS-based filtering provides an additional layer of protection by preventing access to known malicious domains before connections are established, reducing network load and improving response times while blocking threats at the earliest possible point in the communication process. This approach is particularly effective against command-and-control communications and newly identified malicious domains.

5.2 Cloud Integration and Scalability

Cloud-based web filtering services are integrated into the organizational architecture to provide protection for remote users and mobile devices that may not always connect through traditional network infrastructure. These services ensure consistent application of security policies regardless of user location while leveraging global threat intelligence to provide protection against emerging threats.

The architecture is designed to scale dynamically with organizational growth and changing business requirements, incorporating load balancing and redundancy mechanisms that ensure continuous availability of web filtering services. This scalability extends to both on-premises and cloud-based components, providing flexibility to adapt to changing business needs and technology trends.

Integration with existing security infrastructure including Security Information and Event Management systems, Network Access Control solutions, and endpoint protection platforms ensures that web filtering operates as part of a comprehensive security ecosystem rather than as an isolated control, enhancing overall security effectiveness and operational efficiency.

6. Content Categories and Access Control

6.1 Security-Focused Categories

The organization maintains comprehensive categorization of web content to ensure appropriate access controls are applied based on security risk and business requirements. Security-focused categories include malicious content such as malware hosting sites, phishing websites, and command and control servers that pose direct threats to organizational systems and data. These categories are subject to automatic blocking with no exceptions to ensure maximum protection against known threats.

High-risk categories encompass content that may not be directly malicious but presents significant security risks, including anonymous proxy services, peer-to-peer file sharing platforms, and websites hosting hacking tools or security exploits. Access to these categories is generally restricted with limited exceptions available only through formal business justification and enhanced monitoring.

Suspicious and newly registered domains are subject to additional scrutiny and may be blocked pending reputation analysis, ensuring that the organization is protected against emerging threats that have not yet been categorized by traditional security intelligence sources.

6.2 Business and Productivity Categories

Business-related content categories are managed to balance productivity requirements with security considerations, recognizing that some content may be necessary for legitimate business purposes while potentially impacting productivity if accessed excessively. Social networking platforms, entertainment services, and personal communication tools are managed through time-based restrictions and user group policies that allow appropriate access while preventing abuse.

Bandwidth-intensive categories including video streaming services, large file downloads, and cloud storage platforms are subject to bandwidth management controls that ensure adequate network capacity remains available for business-critical applications while allowing reasonable access to these services during appropriate times.

Professional development and educational content are generally permitted and encouraged, supporting the organization's commitment to employee growth and skill development while ensuring that such access aligns with business objectives and does not interfere with work responsibilities.

6.3 Compliance and Legal Categories

Content categories related to legal and regulatory compliance are strictly controlled to ensure the organization meets its obligations under applicable laws and regulations. Adult content, hate speech, discriminatory material, and content depicting violence or illegal activities are blocked to maintain a professional work environment and prevent potential legal liability.

Intellectual property considerations are addressed through controls that prevent access to copyright infringement sites, unauthorized software distribution platforms, and other content that could expose the organization to legal risks related to intellectual property violations.

Workplace conduct categories are managed to support the organization's commitment to maintaining a respectful and inclusive work environment, with controls that prevent access to content that could contribute to harassment, discrimination, or other inappropriate workplace behaviors.

---

7. User Access Management

7.1 Role-Based Access Framework

The organization implements a role-based access control framework that aligns web filtering policies with job responsibilities and business requirements. Executive leadership receives enhanced access privileges that support their strategic responsibilities while maintaining appropriate monitoring and accountability measures to ensure that increased access is used appropriately and in accordance with organizational policies.

Management personnel are granted access levels that support their supervisory responsibilities and business development activities, including access to professional networking platforms and industry resources that may be restricted for general users. This access is balanced with additional accountability measures and regular review processes to ensure continued appropriateness.

Technical staff members receive specialized access that supports their professional responsibilities, including access to security research sites, technical documentation, and development resources that may be restricted for other user groups. This access is accompanied by enhanced monitoring and specific training requirements that ensure technical privileges are used appropriately.

7.2 Dynamic Access Control

The access control framework incorporates dynamic elements that adjust filtering policies based on time of day, location, and current business activities. During business hours, access to entertainment and social media content may be restricted or limited, while outside of normal business hours, these restrictions may be relaxed to support work-life balance and employee satisfaction.

Location-based controls ensure that users accessing organizational networks from different geographic locations receive appropriate filtering policies that comply with local regulations and security requirements while maintaining consistency with organizational standards and expectations.

Project-based access modifications allow temporary adjustments to filtering policies to support specific business initiatives or research activities, with appropriate approval processes and time limitations that ensure such modifications do not create ongoing security risks or policy violations.

---

8. Monitoring and Compliance Framework

8.1 Comprehensive Monitoring Strategy

The organization implements comprehensive monitoring of web filtering activities to ensure policy compliance, detect security threats, and support incident investigation and forensic analysis. This monitoring encompasses all web traffic passing through organizational networks, with detailed logging of user activities, blocked content attempts, and policy violations.

Real-time monitoring capabilities enable immediate detection and response to security threats, policy violations, and system performance issues. Automated alerting systems notify security personnel of critical events, enabling rapid response to potential security incidents and ensuring that threats are addressed before they can impact organizational operations.

Trend analysis and behavioral monitoring help identify patterns that may indicate security threats, policy violations, or opportunities for policy optimization. This analysis supports continuous improvement of web filtering effectiveness while identifying training needs and policy adjustment requirements.

8.2 Privacy and Legal Considerations

Monitoring activities are conducted in accordance with applicable privacy laws and employment regulations, ensuring that employee privacy rights are respected while maintaining the necessary level of security oversight. Clear notification is provided to all users regarding the scope and purpose of monitoring activities, ensuring transparency and compliance with legal requirements.

Data retention policies for monitoring logs balance the need for security investigation capabilities with privacy considerations and storage costs, establishing appropriate retention periods that support business and legal requirements while minimizing privacy impact and storage overhead.

Access to monitoring data is strictly controlled and limited to authorized personnel with legitimate business needs, ensuring that sensitive information collected through monitoring activities is protected and used only for appropriate purposes such as security investigation and policy enforcement.

---

9. Incident Response and Violation Management

9.1 Incident Classification and Response

The organization maintains a structured approach to incident response that addresses both security incidents detected through web filtering systems and policy violations by users. Security incidents including malware detection, phishing attempts, and command and control communications trigger immediate response procedures that include threat containment, investigation, and remediation activities.

Policy violations are classified based on severity and intent, with minor violations such as accidental access to blocked content addressed through user education and counseling, while major violations involving intentional circumvention of security controls or access to prohibited content result in formal disciplinary action and enhanced monitoring.

Severe violations that involve malicious activities, legal violations, or repeated policy breaches may result in immediate account suspension, law enforcement notification, and termination of employment or contract relationships, depending on the nature and severity of the violation.

9.2 Investigation and Documentation

Investigation procedures ensure that all incidents and violations are thoroughly documented and analyzed to determine root causes, assess impact, and identify opportunities for improvement. This includes preservation of evidence, interview of relevant personnel, and analysis of system logs and monitoring data.

Documentation standards ensure that investigation findings are recorded in a manner that supports potential legal proceedings, regulatory reporting, and internal disciplinary actions while maintaining confidentiality and protecting sensitive information related to the investigation process.

Lessons learned from incidents and violations are incorporated into policy updates, training programs, and system improvements to prevent similar occurrences and enhance the overall effectiveness of web filtering controls and organizational security posture.

---

10. Performance Management and Optimization

10.1 Performance Metrics and Measurement

The organization establishes comprehensive performance metrics that measure the effectiveness of web filtering controls in protecting against security threats, supporting business productivity, and maintaining compliance with organizational policies. These metrics include threat detection rates, false positive rates, system availability, and user satisfaction measures.

Security effectiveness is measured through analysis of blocked threats, prevented security incidents, and successful protection against emerging attack vectors. This analysis helps demonstrate the value of web filtering investments while identifying areas where additional protection or policy adjustments may be needed.

Operational performance metrics including system response times, throughput capacity, and availability ensure that web filtering controls do not negatively impact business productivity or user experience while providing the necessary level of security protection.

10.2 Continuous Improvement Process

Regular performance reviews analyze web filtering effectiveness and identify opportunities for improvement in technology, policies, and procedures. These reviews incorporate feedback from users, security teams, and business stakeholders to ensure that web filtering controls continue to meet evolving business and security requirements.

Technology assessments evaluate new web filtering capabilities, threat intelligence sources, and integration opportunities that could enhance security protection or operational efficiency. These assessments support strategic planning for web filtering infrastructure and ensure that the organization remains current with evolving security technologies.

Policy optimization activities analyze usage patterns, violation trends, and business feedback to identify opportunities for policy refinement that better balance security protection with business productivity and user satisfaction requirements.

---

11. Training and Awareness Program

11.1 Comprehensive Training Framework

The organization implements comprehensive training programs that ensure all personnel understand their responsibilities regarding appropriate internet usage and web filtering policies. New employee orientation includes detailed coverage of web filtering policies, acceptable use guidelines, and security awareness fundamentals that establish clear expectations from the beginning of employment.

Ongoing training programs address evolving threats, policy updates, and best practices through regular awareness sessions, online training modules, and targeted communications. These programs are tailored to different user groups and roles, ensuring that training content is relevant and actionable for each audience.

Specialized training for technical staff, managers, and security personnel provides detailed knowledge of web filtering technologies, investigation procedures, and policy enforcement responsibilities that support effective implementation and management of web filtering controls.

11.2 Awareness and Communication Strategy

Regular communication campaigns reinforce web filtering policies and security awareness through multiple channels including newsletters, intranet postings, and team meetings. These communications highlight emerging threats, policy reminders, and success stories that demonstrate the value of web filtering controls.

Interactive awareness activities including simulated phishing exercises, security workshops, and policy quiz competitions engage users and reinforce learning while providing opportunities to assess the effectiveness of training programs and identify areas for improvement.

Feedback mechanisms enable users to report issues, suggest improvements, and seek clarification regarding web filtering policies and procedures, supporting continuous improvement and ensuring that policies remain practical and effective in real-world business environments.

---

12. Technology Management and Administration

12.1 System Administration Framework

Web filtering systems are managed through standardized administration procedures that ensure consistent configuration, optimal performance, and effective security protection. Configuration management processes maintain baseline configurations, track changes, and ensure that modifications are properly tested and documented before implementation.

Regular maintenance activities including software updates, performance tuning, and capacity planning ensure that web filtering systems continue to operate effectively as business requirements and threat landscapes evolve. These activities are scheduled to minimize business impact while maintaining security effectiveness.

Integration management ensures that web filtering systems operate effectively with other security technologies and business applications, providing seamless user experience while maintaining comprehensive security protection across the organizational technology environment.

12.2 Vendor and Technology Management

Vendor relationships are managed to ensure continued support, technology updates, and alignment with organizational security requirements. Regular vendor reviews assess performance, support quality, and strategic alignment while identifying opportunities for improvement or alternative solutions.

Technology roadmap planning ensures that web filtering capabilities evolve with business requirements and threat landscapes, incorporating new technologies and capabilities that

enhance security protection while supporting business productivity and operational efficiency.

Contract management activities ensure that vendor agreements include appropriate service level commitments, security requirements, and support provisions that meet organizational needs while providing flexibility to adapt to changing requirements and technologies.

---

13. Business Continuity and Risk Management

13.1 Continuity Planning and Resilience

The organization implements comprehensive business continuity planning for web filtering services to ensure that security protection remains effective during disruptions and that business operations can continue with minimal impact. This includes redundant system architectures, geographic distribution of filtering infrastructure, and automated failover capabilities.

Disaster recovery procedures ensure that web filtering services can be restored quickly following major disruptions, with documented recovery procedures, tested backup systems, and clear responsibilities for recovery activities. These procedures are regularly tested and updated to ensure effectiveness and alignment with business requirements.

Risk assessment activities identify potential threats to web filtering services including technology failures, cyber-attacks, and vendor disruptions, with appropriate mitigation strategies and contingency plans that ensure continued security protection and business operations.

13.2 Risk Management Integration

Web filtering risk management is integrated into the organization's overall risk management framework, ensuring that web-based threats and filtering control effectiveness are considered as part of comprehensive risk assessment and treatment activities.

Regular risk assessments evaluate the effectiveness of web filtering controls in addressing identified threats and vulnerabilities, with updates to filtering policies and technologies as needed to address evolving risks and maintain appropriate protection levels.

Risk communication ensures that business stakeholders understand web-based risks and the role of filtering controls in risk mitigation, supporting informed decision-making regarding business activities and technology investments that may impact web filtering effectiveness.

---

14. Audit and Compliance Assurance

14.1 Internal Audit Framework

The organization conducts regular internal audits of web filtering controls to ensure compliance with policies, effectiveness of security protection, and alignment with business requirements. These audits include review of system configurations, policy compliance, incident response effectiveness, and user training completion.

Audit procedures are designed to provide comprehensive assessment of web filtering program effectiveness while identifying opportunities for improvement and ensuring that controls remain appropriate for current business and threat environments.

Audit findings are documented and tracked through formal remediation processes that ensure identified issues are addressed promptly and effectively, with follow-up activities that verify the effectiveness of corrective actions and prevent recurrence of similar issues.

14.2 External Compliance Support

The organization maintains documentation and evidence necessary to support external audits and regulatory examinations, ensuring that web filtering controls can be demonstrated to meet applicable compliance requirements and industry standards.

Compliance reporting activities provide regular updates to management and external stakeholders regarding web filtering program effectiveness, compliance status, and continuous improvement activities that demonstrate ongoing commitment to security excellence.

Regulatory change monitoring ensures that web filtering policies and procedures remain current with evolving compliance requirements, with timely updates to controls and procedures as needed to maintain compliance and avoid regulatory violations.

---

15. Governance and Accountability

15.1 Governance Structure

Web filtering governance is integrated into the organization's overall information security governance framework, with clear roles and responsibilities for policy development, implementation oversight, and performance management. Executive leadership provides strategic direction and resource allocation while ensuring that web filtering controls align with business objectives and risk tolerance.

The Information Security Committee provides oversight of web filtering policy development and implementation, with regular reviews of program effectiveness, policy updates, and

strategic planning activities that ensure continued alignment with organizational needs and industry best practices.

Operational governance includes regular management reviews of web filtering performance, incident trends, and user feedback that support continuous improvement and ensure that controls remain effective and appropriate for current business environments.

15.2 Accountability and Responsibility

Clear accountability structures ensure that all stakeholders understand their responsibilities regarding web filtering compliance, from individual users who must comply with acceptable use policies to technical staff who maintain filtering systems and managers who enforce policy compliance.

Performance measurement and reporting provide visibility into web filtering program effectiveness and individual compliance with policies, supporting accountability and enabling recognition of good performance while identifying areas where additional support or corrective action may be needed.

Regular review and update processes ensure that governance structures and accountability mechanisms remain effective as the organization evolves and web filtering requirements change, maintaining clear lines of responsibility and effective oversight of program activities.

---

16. Document Control and Maintenance

16.1 Policy Lifecycle Management

This policy is subject to regular review and update to ensure continued relevance and effectiveness in addressing evolving business requirements, threat landscapes, and regulatory obligations. Annual comprehensive reviews assess all aspects of the policy while quarterly updates address urgent changes and emerging requirements.

Change management procedures ensure that policy modifications are properly evaluated, approved, and communicated to affected stakeholders, with appropriate training and awareness activities that support effective implementation of policy changes.

Version control and documentation management ensure that current policy versions are readily available to all stakeholders while maintaining historical records that support audit activities and demonstrate the evolution of organizational web filtering requirements and controls.

16.2 Communication and Distribution

Policy communication strategies ensure that all affected personnel are aware of current requirements and any changes to web filtering policies, with multiple communication channels and formats that accommodate different learning styles and organizational roles.

Distribution management ensures that policy documents are readily accessible to all stakeholders while maintaining appropriate access controls and version management that prevent confusion and ensure that users are working with current policy requirements.

Feedback mechanisms enable continuous improvement of policy content and presentation, ensuring that policies remain clear, practical, and effective in supporting organizational security objectives while meeting the needs of diverse stakeholder groups.

---

17. Performance and Metrics

17.1 Key Performance Indicators

17.1.1 Security Metrics

Metric	*Target*	*Measurement*	*Frequency*
Malware Blocked	≥ 99.5%	Blocked threats / Total threats detected	Daily
Phishing Blocked	≥ 99%	Blocked phishing / Total phishing attempts	Daily
Policy Violations	≤ 5% of users/month	Users with violations / Total users	Monthly
False Positives	≤ 1%	Incorrectly blocked / Total blocks	Weekly
System Availability	≥ 99.9%	Uptime / Total time	Monthly

17.1.2 Performance Metrics

Metric	Target	Measurement	Frequency
Response Time	≤ 100ms	Average web request processing time	Hourly
Throughput	≥ 95% of baseline	Current throughput / Baseline throughput	Hourly
Bandwidth Utilization	≤ 80%	Used bandwidth / Available bandwidth	Continuous
User Satisfaction	≥ 85%	Positive feedback / Total feedback	Quarterly

17.1.3 Compliance Metrics

Metric	Target	Measurement	Frequency
Policy Compliance	≥ 95%	Compliant users / Total users	Monthly
Training Completion	≥ 98%	Completed training / Required training	Quarterly
Exception Approval	≤ 48 hours	Average exception processing time	Monthly
Audit Findings	≤ 5 per audit	Number of audit findings	Per audit

18. Web Filtering Process

The Web Filtering Process at **[Company name]** is a systematic approach to control and monitor access to internet resources, ensuring a secure and productive online environment. This process is aligned with ISO 27001:2022 Annex A Control 8.23.

18.1 Web Filtering Categories and Rules

Web filtering will be implemented based on predefined categories and rules to block or restrict access to certain types of websites. These categories and rules will be regularly reviewed and updated.

18.1.1 Prohibited Categories

Access to the following categories of websites will generally be prohibited for all users:

- **Malicious Sites:** Websites known for hosting malware, viruses, spyware, ransomware, or other malicious code (e.g., phishing sites, command and control servers).
- **Illegal Content:** Websites containing illegal material, such as child pornography, hate speech, or sites promoting illegal activities.
- **Hacking/Cracking:** Websites providing information or tools related to hacking, cracking, or other unauthorized access activities.
- **Gambling:** Online gambling sites.
- **Adult Content:** Pornographic or sexually explicit content.

18.1.2 Restricted Categories

Access to the following categories of websites may be restricted or monitored, with exceptions granted for legitimate business purposes:

- **Social media:** Social networking sites (e.g., Facebook, Twitter, Instagram) may be restricted during business hours or for specific roles.
- **Streaming Media:** Video and audio streaming sites (e.g., YouTube, Netflix, Spotify) may be restricted due to bandwidth consumption and potential for non-business use.

- **Personal Email/Cloud Storage:** Access to personal webmail services or unauthorized cloud storage platforms may be restricted to prevent data leakage.
- **File Sharing/P2P:** Peer-to-peer file sharing sites and applications.
- **File Sharing/P2P:** Peer-to-peer file sharing sites and applications.

18.1.3 Allowed Categories

Access to websites falling under legitimate business-related categories will generally be allowed. This includes:

- Business-related news and information sites.
- Industry-specific resources and professional development sites.
- Vendor and partner websites are necessary for business operations.

18.2 Implementation of Web Filtering Solutions

[Company name] will deploy and maintain web filtering solutions capable of enforcing the defined categories and rules. These solutions may include:

- **Network-based Web Filters:** Appliances or software deployed at the network perimeter to filter all outbound and inbound web traffic.
- **Cloud-based Web Filters:** Services that route web traffic through a cloud-based security platform for filtering.
- **Endpoint-based Web Filters:** Software agents installed on individual devices to enforce web filtering policies, especially for remote users.
- **DNS Filtering:** Blocking access to malicious domains at the DNS level.

18.3 Web Filtering Process Execution

The web filtering process will involve several key activities:

- **Policy Configuration:** Configuring web filtering solutions with the defined categories, rules, and exception lists.
- **Real-time Blocking:** Automatically blocking access to websites that fall into prohibited categories or are identified as malicious (e.g., known phishing sites, malware distribution sites).
- **Content Inspection:** Inspecting web content for keywords, phrases, or patterns indicative of policy violations or malicious code.
- **URL Blacklisting/Whitelisting:** Maintaining dynamic blacklists of known malicious or inappropriate URLs and whitelists of approved business-critical sites.
- **HTTPS Inspection:** Decrypting and inspecting HTTPS traffic to ensure comprehensive filtering and threat detection, while adhering to privacy regulations.

19. References

- Information Security Policy
- Acceptable Use Policy (AUP)
- Business Continuity Plan
- Incident Response Plan
- Asset Management Policy
- Data Classification and Handling Policy