BROADview NETWORKS

PRODUCTIVITY THROUGH TECHNOLOGY

Powered by **MSP Corp**

CIS 8 Assessment / Microsoft 365 Benchmark - Security Planning

Prepared for: Assembly of Manitoba Chiefs

Prepared by: Nora Rea

Quote #009Q032087 v1

Introduction

Broadview Secure Division

Broadview has strategically focused on developing a security portfolio that will help clients build IT security business plans. To do this we have created a "Broadview Secure" division, aligned our practices to internationally recognized security frameworks, and expanded our team to include certified security specialists. We've also partnered with a Canadian based SOC (security operations centre) providing 24x7 managed security services to many Manitoba customers.

Security Assessments

Given today's cyber threats, security assessments are required for an organization's sustainability. An informed security assessment is the foundation for a Security Business Plan and will...

1. Help identify critical and exploitable weaknesses in your cyber security controls and posture
2. Assist in meeting compliance with industry regulations
3. Improve Management's understanding of current cyber threats and how to counter them
4. Identify a road map for security improvements
5. Provide the business case for security expenditure
6. Strengthen security policies and procedures

A security assessment is part of the journey to improving your overall security posture. The assessment provides the current state of security policies with descriptive guidance on how to take action.

Our security assessments are based on the Centre for Internet Security (CIS) framework. Organizations around the world rely on the CIS Controls best practices to improve their cyber defenses. The CIS Control framework is highly regarded and recommended for a variety of reasons including...

- Expert input: The CIS Controls are monitored by some of the world's leading cybersecurity experts.
- Responsive: The Controls are continually updated based on the changing threat landscape.
- User-friendly: CIS Controls are concise and easy to understand and implement.
- Budget-friendly: The goal is to allow organizations to implement security best practices with limited budget and resources.

Assessment Tables

CIS Security Assessment

The CIS Controls are prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. But this is not a one-size-fits-all solution. Many organizations cannot address all controls based on limited resources. As a result, CIS has organized the controls into three Implementation Groups. The groups are self-assessed categories for organizations based on relevant cybersecurity attributes. Each group identifies a subset of the CIS Controls that the community has broadly assessed to be reasonable for an organization with a similar risk profile and resources to strive to implement. These groups represent a horizontal cut across the CIS Controls. CIS considers Implementation Group 1 (IG1) to be "basic cyber hygiene" that is a minimum standard which all organizations should strive to meet.

CIS Controls		# of Sub-Controls included in the assessment per Group		
Basic Controls		**Group 1**	**Group 2**	**Group 3**
1	Inventory and Control of Enterprise Assets	2	4	5
2	Inventory and Control of Software Assets	3	6	7
3	Data Protection	6	12	14
4	Secure Configuration of Enterprise Assets and Software	7	11	12
5	Account Management	4	6	6
6	Access Control Management	5	7	8
	Subtotal	**27**	**46**	**52**
Foundational Controls				
7	Continuous Vulnerability Management	4	7	7
8	Audit Log Management	3	11	12
9	Email and Web Browser Protections	2	6	7
10	Malware Defenses	3	7	7
11	Data Recovery	4	5	5
12	Network Infrastructure Management	1	7	8
13	Network Monitoring and Defense	0	6	11
14	Security Awareness and Skills Training	8	9	9
15	Service Provider Management	1	4	7
16	Application Software Security	0	11	14
	Subtotal	**26**	**73**	**87**
Organizational Controls				
17	Incident Response Management	3	8	9
18	Penetration Testing	0	3	5
	Subtotal	**3**	**11**	**14**
	Total	**56**	**130**	**153**

Microsoft 365 Benchmark Security Assessment

The CIS Security Benchmark for Microsoft 365 provides prescriptive guidance for establishing a secure configuration posture for Microsoft /Office 365 running on any OS and includes Exchange Online, SharePoint Online, OneDrive for Business, Teams, Azure Active Directory, and inTune. Assessments are tailored to the type of Microsoft licensing the customer is currently subscribed to based on 4 levels as described below. Many environments have a mix of license types that may overlap into multiple levels. The levels are a guide and not a strict list.

- **E3 Level 1**: These organizations mostly run Microsoft 365 Business Basic, Standard, or Premium or Office 365 E1 to E3 and desire a practical and prudent approach to security.
- **E3 Level 2:** These organizations mostly run Microsoft 365 Business Premium or Office 365 E3 and consider security paramount.
- **E5 Level 1:** These organizations mostly run Microsoft 365 E5 or Office 365 E5 and desire a practical and prudent approach to security.
- **E5 Level 2:** These organizations mostly run Microsoft 365 E5 or Office 365 E5 and consider security paramount.

Microsoft 365 CIS Benchmark		Unique Sub-Controls Per Level			
		E3 Level 1	E3 Level 2	E5 Level 1	E5 Level 2
1	Azure Active Directory	11	5	1	3
2	Application Permissions	3	4	0	3
3	Data Management	2	4	1	1
4	Email Security / Exchange Online	8	4	1	2
5	Auditing	12	1	1	1
6	Storage	1	3	0	0
7	Mobile Device Management	11	2	0	0
	Unique Sub-Controls per Level:	**48**	**23**	**4**	**10**
	Plus Required Level(s):	**0**	**48 (E31)**	**48 (E31)**	**48 (E31) + 4 (E51)**
	Total Sub-Controls:	**48**	**71**	**52**	**62**

CIS 8 Assessment / Microsoft 365 Benchmark - Security Planning

Quote Information:

Quote #: 009Q032087
Version: 1
Delivery Date: 11/16/2023
Expiration Date: 12/14/2023

Prepared for:

Assembly of Manitoba Chiefs
200-275 Portage Ave
Winnipeg, MB R3B 2B3
Howard Burston
hburston@manitobachiefs.com
(204) 956-0610

Prepared by:

Broadview Networks
Nora Rea
(204) 984-9897
Fax
nrea@broadviewnetworks.ca

Bill To

Assembly of Manitoba Chiefs
ATTN: Howard Burston
200-275 Portage Ave
Winnipeg, MB R3B 2B3

Ship To

Assembly of Manitoba Chiefs
ATTN: Howard Burston
200-275 Portage Ave
Winnipeg, MB R3B 2B3

Payment Options		Periods	Payments	Amount
Payment Terms				
Net Terms	One-Time Payments	One-Time	1	$9,004.80
Credit Card	One-Time Payments	One-Time	1	$9,139.87

Summary of Selected Payment Options	Amount
Payment Terms: Net Terms	
Total of One-Time Payments	$9,004.80

Services Terms: Fixed Fee work is progress billed monthly based on the % of work attributed to that month - Time & Material work is typically billed weekly or monthly - Services are delivered during normal business hours. After hour rates may apply for evening or weekend work - Travel outside of Winnipeg is subject to millage and travel time fees.

Invoices payable by customer cheque or electronic funds transfers by due date. 1.5% monthly is applied to overdue accounts. Subject to approved terms and account in good standing. Net Terms are presented at our cash discounted rate.

Security Terms & Conditions

Applicable to Security Services

Should a Statement of Work include security scanning, testing, assessment, forensics, or remediation Services ("Security Services"), Client understands that Broadview Networks may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. Client authorizes Broadview Networks to perform such Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services or otherwise approved by Client from time to time) on network resources with the IP Addresses identified by Client. Client represents that, if Client does not own such network resources, it will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Broadview Networks, to permit Broadview Networks to provide the Security Services. Broadview Networks shall perform Security Services during a timeframe mutually agreed upon with Client. The Security Services, such as penetration testing or vulnerability assessments, may also entail buffer overflows, fat pings, operating system specific exploits, and attacks specific to custom coded applications but will exclude intentional and deliberate Denial of Service Attacks. Furthermore, Client acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding the Client's systems and accepts those risks and consequences. Client hereby consents and authorizes Broadview Networks to provide any or all the Security Services with respect to the Client's systems. Client further acknowledges it is the Client's responsibility to restore network computer systems to a secure configuration after Broadview Networks Consultant testing.

Applicable to Compliance Services

Should a Statement of Work include compliance testing or assessment or other similar compliance advisory Services ("Compliance Services"), Client understands that, although Broadview Networks' Compliance Services may discuss or relate to legal issues, Broadview Networks does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Client is ultimately responsible for retaining its own legal counsel to provide legal advice, Furthermore, any written summaries or reports provided by Broadview Networks in connection with any Compliance Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Client's legal or regulatory compliance. Furthermore, any outcome of the services involving compliance assessment is limited to a point-in-time examination of the Client's compliance or non-compliance status with the applicable standards or industry best practices set forth in the Scope of Work and that the outcome of any audits, assessments, or testing by, and the opinions, advice, recommendations, and/or certification by Broadview Networks does not constitute any form of representation, warranty, or guarantee that Client's systems are 100% secure from every form of attack. In assisting in the examination of Client's compliance or non-compliance status, Broadview Networks relies upon accurate, authentic, and complete information provided by Client, as well as use of certain sampling techniques.

MASTER SERVICES AGREEMENT SOW.2021.1

THIS AGREEMENTmade on November 16, 2023.

B E T W E E N: Assembly of Manitoba Chiefs(the "**Client**") , and **MSP OPERATIONAL CORP.** (dba **BROADVIEW NETWORKS**) a corporation incorporated pursuant to the laws of Manitoba (the "**Consultant**")

WHEREASthe Consultant is in the business of providing information technology services to its customers;

AND WHEREASthe Client wishes to retain the Consultant to provide the Client with certain information technology services, all as more particularly described in this Agreement;

NOW THEREFORE THIS AGREEMENT WITNESSESthat in consideration of the respective covenants and agreements of the parties contained herein, the sum of one ($1.00) dollar paid by each party to the other, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

ARTICLE 1-INTERPRETATION

1.1 Definitions. In this Agreement, unless the context otherwise requires, the following terms have the following meanings:

(a) "**Addendum**" means the agreement attached hereto as Schedules, as amended or modified between the parties from time to time, which describes a Service to be provided by the Consultant to the Client and any additional terms and conditions relating specifically to that Service;

(b) "**Business Day**" means any day, other than Saturday, Sunday or any statutory holiday in the Province of Manitoba;

(c) "**Deliverables**" means the documentation and reports to be prepared by the Consultant and delivered to the Customer as set out in the Statement of Work;

(d) "**Confidential Information**" means any business, marketing, technical, scientific, proprietary or other information disclosed by a party and relating to such party's operations, products, designs, plans, strategy, customers, business opportunities, finances, technology, research, development, processes, know-how, trade secrets or other intellectual property, or relating to the employees, customers or suppliers of a party, and, at the time of disclosure, is designated as confidential, is disclosed in circumstances of confidence, or would be understood by the receiving party, exercising reasonable business judgment, to be confidential, but does not include any information which is or becomes available to the public through no fault of the other party or which is disclosed to the other party by a third party who has lawfully obtained such information and owes no obligation of confidentiality with respect to such information;

(e) "**Fees**" means the fees to be paid by the Client to the Consultant as set out in a Statement of Work;

(f) "**Services**" means the services to be performed by the Consultant as set out in a Statement of Work; and

(g) "**Statement of Work**" means a statement of work, attached hereto as a Schedule or executed by the parties hereto, as the same may be amended from time to time by the parties hereto in writing, which shall form a part of and be governed by the terms and conditions contained in this Agreement.

ARTICLE 2-SERVICES

2.1 Engagement. Subject to the terms of this Agreement, the applicable Statement of Work and any applicable Addendum, the Client hereby retains the Consultant, and the Consultant hereby accepts the engagement, to provide the Services set out in each Statement of Work.

2.2 Change Order.

(a) If the Client wishes at any time to request a change in the Services under a Statement of Work, or if the Client requests that the Consultant provide services outside the scope of the Services, the Client will, unless otherwise agreed between the Client and the Consultant, prepare a written change request. The Consultant will evaluate and respond to any change request promptly and will advise the Client in writing of any impact on the cost of and delivery schedule for any Services as a result of the proposed change. Upon confirmation from the Client, the parties shall execute a change order form setting out the agreed upon changes, and the Statement of Work shall be deemed to have been amended in accordance with the change order form.

(b) If the Consultant determines that an assumption in a Statement of Work is inaccurate, and such inaccuracy impacts the cost and/or delivery schedule of the Services under such Statement of Work, the Consultant shall submit a change order form to the Client setting out proposed changes to such Statement of Work based on a modified, accurate assumption. Upon confirmation from the Client that the modified assumption is accurate and the Consultant?s proposed changes are acceptable, the parties shall execute the change order form and the Statement of Work shall be deemed to have been amended in accordance with the change order form.

(c) The Consultant will have no obligation to implement a change in the Services under a Statement of Work unless such change is first agreed upon in writing by the Client and the Consultant in a change order form.

(d) The parties agree to use the change order form set out in Schedule ?B?.

2.3 Delays. If the timetable for the performance of any Services is delayed as a result of a delay by the Client in the performance of its responsibilities as set out herein or in a Statement of Work, or as the result of any change in the Services to which the Consultant and the Client have agreed, or as the result of any factor which is beyond the reasonable control of the Consultant, then the timetable for the performance of the Services shall be extended for the period of time that the Services have been delayed as a result of such factor or events.

2.4 Client Responsibilities. The Client will be responsible for the following, in addition to any specific responsibilities set out in a Statement of Work:

(a) respond to requests for relevant information on a timely basis;

(b) if applicable, ensure that sufficient Client representatives are present as the Consultant may reasonably require in connection with the performance of the Services;

(c) provide the Consultant with timely and accurate information and documentation, as reasonably required by the Consultant to perform the Services;

(d) if applicable, make available to the Consultant personnel familiar with the Client?s requirements and with the expertise necessary to permit the Consultant to provide the Services;
(e) maintain a proper operating environment for software and hardware, if the maintenance of such proper operating environment may affect the performance of

the Services;

(f) if applicable, provide a safe area for the Consultant to perform the Services;

(g) purchase for ownership or license, as applicable, all hardware and software set out in each applicable Statement of Work, or as otherwise agreed upon by the parties from time to time, for the purposes of the Consultant performing the Services;

(h) review work in process on a regular basis and provide feedback to the personnel assigned by the Consultant on in-process and completed work;

(i) provide the Consultant with a signed document specifying acceptance of the Services, or deficiencies noted, within five (5) Business Days from the date on which the Services are completed, unless otherwise noted;

(j) notify the Consultant in writing of any concerns or noted deficiencies of work performed by the Consultant?s personnel to facilitate correction or adjustment to the work;

(k) ensure that the Client?s personnel assigned to the project are available as scheduled; and

(l) pay the Consultant the Fees as set out in the Statement of Work.

2.5 Representations and Warranties. The Consultant represents and warrants that:

(a) the Consultant and any personnel who may be assigned by the Consultant to perform the Services possess the necessary skills, expertise and experience to provide the Services in accordance with the provisions of this Agreement;

(b) the Consultant and any personnel who may be assigned by the Consultant to perform the Services shall be fully licensed by all industry, professional and government agencies as may be required to perform the Services, and in the performance of the Services, shall comply in all material respects with the terms and conditions of such licences;

(c) the Consultant shall maintain Workers Compensation Board of Manitoba coverage as required by law; and

(d) the Consultant shall maintain a comprehensive general liability insurance policy with coverage for any one occurrence or claim of not less than 2 million dollars ($2,000,000).

2.6 Right to Subcontract. The Consultant may, without the written consent of the Client, subcontract to any third party any of the Services provided by the Consultant to the Client hereunder. In the event that the Consultant subcontracts any of the Services to a third party services provider, the Consultant shall be and remain fully responsible for any acts of such subcontractors.

2.7 Relationship Management. The parties acknowledge that cooperation is essential to the successful delivery of the Services and compliance with all other requirements of this Agreement. The parties agree to each appoint a person the primary representative of the party for the administration and other matters relative to the provision of Services, and use mutually agreed processes and forms to report progress and to identify, track and resolve problems. Unless otherwise provided in the Statement of Work, the standard processes and forms of the Consultant will be utilized. Each party may rely on the authority of the other party?s representative provided that neither person shall have the authority to amend or modify this Agreement.

ARTICLE 3-PAYMENT AND EXPENSES

3.1 Payment. In consideration of the Consultant providing the Services, the Client will pay to the Consultant the Fees and any other fees or amounts upon which the Consultant and the Client may agree from time to time in writing.

3.2 Invoices. Unless otherwise set out in a Statement of Work, the Consultant will provide monthly invoices to the Client which invoices shall set out in reasonable detail the Services provided by the Consultant during the period covered by the particular invoice, the Fees due to the Consultant therefore and the taxes applicable in respect of such Fees. Invoices are due and payable by the Client thirty (30) days from the date of the invoice.

3.3 Interest. Any amounts not paid by the Client when due hereunder shall accrue interest at the rate of 18% per annum (1.5% per month).

3.4 Taxes. It is understood and agreed that the Fees are exclusive of all applicable taxes, duties or government levies (collectively referred to as ?taxes?). The Client is responsible for all relevant taxes. Any of such taxes applicable to the Services will be charged by the Consultant and paid by the Client, as contemplated in section 3.2 above.

3.5 Expenses. The Client will reimburse the Consultant for all pre-approved out-of-pocket expenses relating to the provision of the Services by the Consultant, upon the Consultant furnishing to the Client appropriate receipts for all such expenses.

3.6 Early Service. If the Consultant commences any Services prior to the signing of the related Statement of Work, the Client agrees to pay the Consultant charges for such Service in accordance with the terms of the Statement of Work or any amendments in writing thereto.

3.7 Additional Fees. The Client will also be responsible to the Consultant for all fees and charges associated with any additional services or incremental costs incurred by the Consultant in providing the Services caused by the Client?s failure to:

(a) provide accurate data in a prescribed format;

(b) perform any of its obligations under this Agreement; or

(c) provide data at the time required for processing.

ARTICLE 4-LIMITED WARRANTY

4.1 Limited Warranty. The Consultant warrants to the Client that the Consultant shall use commercially reasonable efforts to provide the Services in accordance with all generally accepted industry standards applicable to the provision of similar services. OTHER THAN AS EXPRESSLY STATED IN THIS AGREEMENT, THE CONSULTANT SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR FUNCTION.

4.2 No Liability. Notwithstanding anything herein contained to the contrary, in no event whatsoever will the Consultant, its directors, officers, shareholders, employees, agents, representatives, contractors or affiliates, be liable for any claim for:

(a) punitive, exemplary or aggravated damages;

(b) damages for loss of profits or revenue, failure to realize expected savings, loss of use or lack of availability of Prior Products or Developed Products (including computer resources and stored data);

(c) indirect, consequential or special damages of any kind; or

(d) contribution, indemnity or set-off in respect of any claims against the other party by any third party.

4.3 Negligence. Notwithstanding sections 4.1 and 4.2, the Consultant shall not be liable for any losses or damages caused by the negligence of the Consultant, or any of its officers, directors, employees, agents and representatives.

4.4 Limitation on Liability. Without limiting the generality of sections 4.1, 4.2 and 4.3, the parties agree that the maximum total liability of the Consultant, its

directors, officers, shareholders, employees, agents, representatives, contractors and affiliates, to the Client, for any claim whatsoever, under any circumstances, regardless of the cause of action and including without limitation claims for breach of contract, tort, indemnification, negligence or otherwise, and the Client?s sole remedy therefore, shall be strictly limited to an award for direct, provable damages not to exceed the amount of Fees paid by the Client to the Consultant under the Statement of Work in respect of which the claim arose.

4.5 Reasonableness of Limitations. The parties agree that the limitations contained in this section 4 are reasonable in scope, that the Consultant would not have entered into this Agreement without the limitations contained in this section 4, and that the terms and conditions of this Agreement have been negotiated taking into account such limitations.

4.6 Exclusions. The Client acknowledges that there are risks inherent in use of the Internet that could result in the loss of privacy, confidential information and property, including any data or information transmitted by any server designated as ?secure?. The Client is solely responsible for the suitability of the Service chosen, and acknowledges that the Service is provided on an ?as is? basis except as expressly stated in this Agreement. The Client confirms that it has not relied on any representation, warranty, condition or promise made by the Consultant which has not been expressly stated in this Agreement.

ARTICLE 5-INDEMNIFICATION

5.1 Indemnities by the Client.

(a) The Client hereby agrees to defend, indemnify and hold the Consultant, its directors, officers, employees, agents, contractors and affiliates, harmless from and against any and all claims, losses, damages, liabilities or expenses, including reasonable legal costs, that any of them may incur as a result of or in connection with any breach by the Client of any of its obligations under this Agreement.

(b) The Client hereby agrees to defend, indemnify and hold the Consultant, its directors, officers, employees, agents, contractors and affiliates, harmless from and against any and all claims of infringement made against the Consultant for any patent, copyright, trade-mark, service mark, trade name or other proprietary rights in regard to any products or materials of the Client accessed or used in the performance of the Services, or otherwise under this Agreement.

ARTICLE 6-INTELLECTUAL PROPERTY RIGHTS AND PRIVACY

6.1 Developed Products. All original materials, data, computer code, specifications, discs and programs, either in written or in magnetic or electronic form, which are prepared or produced by the Consultant specifically for the Client under this Agreement (as contemplated in a Statement of Work), and which are fully paid for by the Client, shall be or become the sole property of the Client (?Developed Products?). The Client hereby grants the Consultant and its affiliates (and any of their contractors) a non-exclusive, perpetual, fully paid-up license to use, reproduce and modify any and all Developed Products for any purpose whatsoever.

6.2 Prior Products. All materials, data, computer code, specifications, discs and programs utilized or developed by either party prior to the effective date of this Agreement or created independently of this Agreement shall remain the sole property of the party who has created it (?Prior Products?). During the term of this Agreement, each party grants to the other party and any of such other party?s affiliates (and to their contractors, as necessary) a temporary, non-exclusive license to use, reproduce and modify the Prior Products of the other party solely for the purposes of fulfilling their obligations under this Agreement. Upon payment in full by the Client to the Consultant of all amounts due and owing under this Agreement, and subject to the Consultant?s compliance with the terms of this Agreement (including all terms which survive the termination of this Agreement), the Consultant will grant the Client and its affiliates a non-exclusive, perpetual, fully paid up license to use, reproduce and modify the Prior Products of the Consultant in the form delivered to the Client in connection with this Agreement during the term of this Agreement, solely for the purposes of the Client supporting its own internal business operations.

6.3 Privacy. The parties are each responsible for complying with any obligations applying respectively to them under the applicable data protection and personal information protection laws governing the Client?s data.

ARTICLE 7-CONFIDENTIALITY

7.1 Confidentiality. Except for the purposes of performing its obligations under this Agreement, neither party shall use or disclose any Confidential Information of the other party. A party receiving Confidential Information from the other shall use the same degree of care to protect the confidentiality of such Confidential Information as it uses to protect its own Confidential Information, but in no event less than reasonable care, including ensuring that such information is disclosed to employees and agents on a need to know basis and that all such employees and agents have agreed in writing to similar confidentiality obligations as those contained in this section. Within fifteen (15) days of the request of the disclosing party, and in its sole discretion, the receiving party shall either return to the disclosing party originals and copies of any Confidential Information, or destroy the same. The Consultant shall be permitted to retain a copy of any Client Confidential Information which is either embedded or contained within any documents (physical, electronic or otherwise), records and materials prepared by the Consultant in connection with the Services, or as otherwise required to be retained under applicable law, but such copies will remain subject to the confidentiality obligations set out in this section. Either party may only disclose the general nature, but not the specific terms and conditions, of this Agreement without the prior written consent of the other party. Either party may disclose the Confidential Information of the other party if required to do so by a governmental or regulatory agency or body, but must first notify such other party of the receiving party?s obligations to so disclose (unless prohibited from doing so under applicable law). The disclosure obligations contained herein shall continue for a period of ten (10) years after expiration or termination of this Agreement.

ARTICLE 8-NON-SOLICITATION

8.1 Non-Solicitation. The Client acknowledges that the Consultant is involved in a highly strategic and competitive business. The Client further acknowledges that the Client would gain substantial benefit and that the Consultant would be deprived of such benefit, if the Client were to directly hire any personnel employed by the Consultant. Except as otherwise provided by law, the Client shall not, without the prior written consent of the Consultant, solicit the employment of the Consultant?s personnel or induce any of the Consultant?s personnel to leave to go to another firm during the term of this Agreement and for a period of one (1) year following the termination or expiration of this Agreement. The Client agrees that the Consultant?s damages resulting from breach by the Client of this provision would be impracticable and that it would be extremely difficult to ascertain the actual amount of damages. Therefore, in the event the Client violates this provision, the Client shall immediately pay the Consultant an amount equal to $50,000 as liquidated damages and the Consultant shall have the option to terminate this Agreement without further notice or liability to the Client. The amount of the liquidated damages reflected herein is not intended as a penalty and is reasonably calculated based upon the projected costs the Consultant would incur to identify, recruit, hire and train suitable replacements for such personnel.

ARTICLE 9-CANADIAN ANTI-SPAM LEGISLATION

9.1 Commercial Electronic Messages. The Client, by signing this agreement, acknowledges that it implies consent to Broadview Networks, 1 - 1530 Taylor Avenue, Winnipeg, MB R3N 1Y1, (204) 984-9897, to email messages that encourage participants in a commercial activity. The Client may unsubscribe at any time by emailing its request to unsubscribe to the Consultant at solutions@broadviewnetworks.ca or by clicking ?unsubscribe? in any commercial electronic message.

ARTICLE 10-ADDENDUMS

10.1 Required for certain offerings. The Addendum(s) attached hereto as

Schedules form part of this Agreement.

ARTICLE 11-TERM AND TERMINATION

11.1 Term. The term of this Agreement shall be for a period of one (1) year, or as otherwise set out in any Statement of Work or Addendum, commencing on the date set out above unless terminated in accordance with the provisions of this Agreement. This Agreement may be extended or renewed by agreement of the parties in writing at least ninety (90) days prior to the end of the term.

11.2 Termination with Cause. Without limiting any other rights or remedies available to the parties, at law, in equity or otherwise, each party has the right to terminate this Agreement:

(a) upon the provision of a written notice of termination to the other party, in the event that such other party is in breach or default of any material obligation under this Agreement and such breach or default continues unrectified for ten (10) Business Days following the provision of written notice of such breach or default to such other party; or

(b) immediately in the event that the other party voluntarily enters into proceedings in bankruptcy, makes an assignment for the benefit of its creditors, is adjudged to be bankrupt or insolvent, a petition is filed against it under a bankruptcy law, corporate reorganization law, or any other law for the relief of debtors, or a receiver, trustee or similar person is appointed with respect to its assets.

11.3 Termination without Cause. Either party may terminate this Agreement at any time without cause upon giving the other party no less than thirty (30) days prior written notice of termination. Notwithstanding the foregoing, in the event of a termination of this Agreement without cause, the term of this Agreement shall be extended until all Services are performed and amounts are paid in full under any and all Statements of Work which are outstanding at the time of the intended termination.

11.4 Suspension of Service. The Consultant will be entitled to suspend the Service without liability if:

(a) the Consultant, acting reasonably, believes that the Service is being used in violation of this Agreement or any applicable law;

(b) the Client is in breach of any material term of this Agreement including, without limitation, failing to pay invoiced amounts in full within 30 days of the invoice; or

(c) the Consultant is requested to do so by any law enforcement or governmental agency.

The Client will not be able to access any files on the Consultant?s servers during a suspension of Service. The Consultant will use commercially reasonable efforts to give the Client advance notice in writing of a suspension of Service unless a law enforcement or governmental agency directs otherwise or suspension without notice is necessary to protect the Consultant or its other customers. A suspension of Service under this subsection will not be considered a breach by the Consultant of the terms of this Agreement.

11.5 Effect of Expiration or Termination. Upon termination of this Agreement for any reason whatsoever:

(a) the Client shall pay to the Consultant all amounts owing to the Consultant in respect of the time period up to and including the date of termination of this Agreement;

(b) each party will return all property in its possession or control belonging to the other party to such other party; and

(c) all obligations under this Agreement that are intended to survive the termination of this Agreement shall survive and continue in full force and effect for the period intended.

ARTICLE 12-DISPUTE RESOLUTION

12.1 Good Faith Negotiations. Should a dispute arise regarding the interpretation or construction of, compliance with, or beach of, the Agreement or its termination, the parties shall meet and negotiate in good faith in an attempt to resolve the dispute.

12.2 Arbitration. If the dispute cannot be resolved through good faith negotiations between the parties within a reasonable time, the parties agree that such dispute shall be submitted to arbitration by either party giving written notice to the other party that the party giving the notice has elected to have the dispute submitted to arbitration. In the event the matter is submitted to arbitration, the parties shall attempt to agree on one (1) arbitrator within five (5) Business Days. If the parties cannot agree on a single arbitrator, the parties shall each, within ten (10) Business Days after notice to arbitrate has been received, give notice to the other nominating one (1) arbitrator on its behalf, and the two (2) arbitrators so nominated shall meet and within ten (10) Business Days of their mutual appointment to nominate a chairperson, and the three (3) arbitrators so nominated shall determine the dispute. If either party fails to nominate an arbitrator or if the two (2) arbitrators fail to agree on the nomination of the chairperson, either party may apply upon notice to the other to a Judge of the Court of Queen's Bench (Manitoba) who shall have jurisdiction to nominate the arbitrator or arbitrators. The decision of any two (2) of the three (3) arbitrators is binding on the parties. The cost of arbitration shall be borne equally by the parties. Except as to matters otherwise provided herein or is otherwise agreed by the parties, the provisions of The Arbitration Act (Manitoba) apply.

ARTICLE 13-GENERAL PROVISIONS

13.1 Relationship. The relationship between the Client and the Consultant will at all times be one of independent contractor and nothing herein shall be construed as implying an employment, partnership or joint venture relationship.

13.2 No Exclusivity. The Client acknowledges that nothing in this Agreement obliges the Consultant to devote all or substantially all of its time or attention to the Service and that nothing shall restrict or prevent the Consultant from entering into agreements with other persons concerning the provision of similar services.

13.3 Equitable Relief. Each party acknowledges and agrees that a breach by it under any of the provisions of ARTICLE 6, ARTICLE 7 or ARTICLE 8 would cause serious and irreparable harm to the other party which could not adequately be compensated for in damages and that such other party shall have the right, in addition to any other rights and remedies existing in its favour, to enforce its rights under such Articles not only by an action or actions for damages, but also by an action or actions for specific performance or injunctive relief.

13.4 Survival. The termination or expiration of this Agreement will not affect the survival and enforceability of any provision of this Agreement which is expressly or impliedly intended to remain in force after such termination or expiration.

13.5 Assignment. This Agreement may not be assigned by either party without the prior written consent of the other party, which consent shall not be unreasonably withheld. Any attempt by a party to assign any of its rights or obligations under this Agreement without the prior written consent of the other party is void and of no effect. Notwithstanding the foregoing, either party may assign its rights and obligations under this Agreement to a third party pursuant to a reorganization, merger or sale of all or substantially all of its assets or a division of its business, provided such third party assignee agrees in writing to be bound by the rights and obligations of the assignor hereunder.

13.6 Time of the Essence. Time shall be of the essence in this Agreement.

13.7 Further Assurances. Each of the parties to this Agreement agrees that it will promptly do, make, execute or deliver, or cause to be done, made, executed or delivered, all such further acts, documents and things as the other party hereto may

reasonably require from time to time for the purpose of giving effect to the provisions of this Agreement and will use reasonable efforts and take all such steps as may reasonably be within its power to implement to its full extent the provisions of this Agreement.

13.8 Governing Law. This Agreement shall be governed by the laws of the Province of Manitoba and the laws of Canada applicable therein.

13.9 Enurement. This Agreement shall enure to the benefit of, and be binding upon, the parties hereto and their respective successors and permitted assigns.

13.10 Force Majeure. Without limiting or restricting the applicability of the law governing frustration of contracts, in the event either party fails to meet any of its obligations under this Agreement within the time prescribed, and such failure shall be caused, or materially contributed to, by force majeure (as defined below), such failure shall be deemed not to be a breach of the obligations of such party under this Agreement, and the time for the performance of such obligations shall be extended accordingly as may be appropriate under the circumstances, provided that:

(a) the party who is unable to meet its obligations due to force majeure provides prompt notice to the other party of the force majeure and its anticipated impact on such party's obligations, which notice may be verbal where written notice is impractical under the circumstances; and

(b) such party takes all reasonable commercial steps to work around the force majeure if possible or, in any event, to minimize the delay arising from the force majeure.

For the purpose of this Agreement, "force majeure" shall mean any acts of God, war, terrorism, natural calamities, strikes or other labour stoppages or disturbances, civil commotions or disruptions, riots, epidemics, acts of government or any competent authority having jurisdiction, or any other legitimate cause beyond the reasonable control of such party, and which, by the exercise of due diligence, such party could not have prevented, but lack of funds on the part of such party shall not be deemed to be a force majeure.

13.11 Independent Legal Advice. It is agreed that each party has read and fully understands this Agreement, and has either received independent legal advice or voluntarily chosen not to receive independent legal advice, as the case may be, in connection with the implications of this Agreement.

13.12 Headings. The inclusion in this Agreement of headings and subheadings is for convenience of reference only and shall not affect the construction or interpretation of this Agreement.

13.13 Contra Proferentum. The parties agree that any rule of construction or doctrine of interpretation, including contra proferentum, construing or interpreting any ambiguity against the drafting party shall not apply.

13.14 Gender and Number. In this Agreement, unless the context otherwise requires, words importing the singular include the plural and vice versa and words importing gender include all genders.

13.15 Currency. Unless otherwise set out in a Statement of Work, all amounts referenced in this Agreement and in a Statement of Work are stated and payable in Canadian currency.

13.16 Invalidity of Provisions. Each of the provisions contained in this Agreement is distinct and severable and a declaration of invalidity or unenforceability of any such provision by a court of competent jurisdiction shall not affect the validity or enforceability of any other provision hereof.

13.17 Entire Agreement. This Agreement and all schedules constitute the entire agreement between the parties pertaining to the subject matter of this Agreement. There are no warranties, representations or agreements between the parties in connection with such subject matter except as specifically set forth in this Agreement and in all schedules. In the event that there is a conflict between this Agreement and a schedule, the terms of the schedule shall govern.

13.18 Modification and Waiver. This Agreement may not be modified unless agreed to in writing by both the Client and the Consultant. No extension of any time limit granted by a party shall constitute an extension of any other time limit or any subsequent instance involving the same time limit. No consent by a party to, nor waiver of, a breach by the other party, whether express or implied, shall constitute a consent to or waiver of or excuse for any other different or subsequent breach, unless such waiver or consent is in writing and signed by the party claimed to have waived or consented. Except as otherwise provided herein, no term or provision hereof shall be deemed waived and no breach excused.

13.19 Notices. Any notice, request, consent or other communication provided, required, or permitted under this Agreement shall be sufficiently given if personally served, or sent by prepaid first class mail or by hand delivery as hereinafter provided, and addressed or sent as follows:

(a) If to the Client

Assembly of Manitoba Chiefs
200-275 Portage Ave
Winnipeg, MB R3B 2B3
Attention: Howard Burston

(b) If to the Consultant

Broadview Networks
1 - 1530 Taylor Avenue
Winnipeg, MB R3N 1Y1
Attention: David Reimer

Any such notice or other communication, if mailed by prepaid first class mail, shall be deemed to have been received on the fourth Business Day after the post marked date thereof, or if delivered by hand shall be deemed to have been received at the time it is delivered to the applicable address set out above for such party to an individual at such address having apparent authority to accept deliveries on behalf of the addressee.

13.20 Counterparts. This Agreement may be signed in counterparts and each of such counterparts shall constitute an original document and such counterparts, when taken together, shall constitute one and the same instrument.

Version SOW.2021.1

CIS Center for Internet Security®

CIS Controls® Version 8

Implementation Groups

The CIS Controls are internationally recognized for bringing together expert insight about threats, business technology, and defensive options into an effective, coherent, and simpler way to manage an organization's security improvement program. But in our experience, organizations of every size and complexity still need more help to get started and to focus their attention and resources.

To that end, we developed Implementation Groups (IGs). IGs are the recommended guidance to prioritize implementation of the CIS Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls. Each IG identifies a set of Safeguards (previously referred to as CIS Sub-Controls), that they need to implement. There are 153 Safeguards in CIS Controls v8.

Every enterprise should start with IG1. IG1 provides effective security value with technology and processes that are generally already available while providing a basis for more tailored and sophisticated action if that is warranted. Building upon IG1, we then identified an additional set of Safeguards for organizations with more resources and expertise, but also greater risk exposure. This is IG2. Finally, the rest of the Safeguards make up IG3.

These IGs provide a simple and accessible way to help organizations of different classes focus their scarce security resources, and still leverage the value of the CIS Controls program, community, and complementary tools and working aids.

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Total Safeguards **153**

Basic Cyber Hygiene

CIS Controls v8 defines Implementation Group 1 (IG1) as basic cyber hygiene and represents an emerging minimum standard of information security for all enterprises. IG1 is the on-ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

For more information, visit www.cisecurity.org/controls.

CIS Controls®
Version 8

Number	Control/Safeguard	IG1	IG2	IG3
01	**Inventory and Control of Enterprise Assets**			
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●
02	**Inventory and Control of Software Assets**			
2.1	Establish and Maintain a Software Inventory	●	●	●
2.2	Ensure Authorized Software is Currently Supported	●	●	●
2.3	Address Unauthorized Software	●	●	●
2.4	Utilize Automated Software Inventory Tools		●	●
2.5	Allowlist Authorized Software		●	●
2.6	Allowlist Authorized Libraries		●	●
2.7	Allowlist Authorized Scripts			●
03	**Data Protection**			
3.1	Establish and Maintain a Data Management Process	●	●	●
3.2	Establish and Maintain a Data Inventory	●	●	●
3.3	Configure Data Access Control Lists	●	●	●
3.4	Enforce Data Retention	●	●	●
3.5	Securely Dispose of Data	●	●	●
3.6	Encrypt Data on End-User Devices	●	●	●
3.7	Establish and Maintain a Data Classification Scheme		●	●
3.8	Document Data Flows		●	●
3.9	Encrypt Data on Removable Media		●	●
3.10	Encrypt Sensitive Data in Transit		●	●
3.11	Encrypt Sensitive Data at Rest		●	●
3.12	Segment Data Processing and Storage Based on Sensitivity		●	●
3.13	Deploy a Data Loss Prevention Solution			●
3.14	Log Sensitive Data Access			●

Number	Control/Safeguard	IG1	IG2	IG3
04	**Secure Configuration of Enterprise Assets and Software**			
4.1	Establish and Maintain a Secure Configuration Process	●	●	●
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	●	●	●
4.3	Configure Automatic Session Locking on Enterprise Assets	●	●	●
4.4	Implement and Manage a Firewall on Servers	●	●	●
4.5	Implement and Manage a Firewall on End-User Devices	●	●	●
4.6	Securely Manage Enterprise Assets and Software	●	●	●
4.7	Manage Default Accounts on Enterprise Assets and Software	●	●	●
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		●	●
4.9	Configure Trusted DNS Servers on Enterprise Assets		●	●
4.10	Enforce Automatic Device Lockout on Portable End-User Devices		●	●
4.11	Enforce Remote Wipe Capability on Portable End-User Devices		●	●
4.12	Separate Enterprise Workspaces on Mobile End-User Devices			●
05	**Account Management**			
5.1	Establish and Maintain an Inventory of Accounts	●	●	●
5.2	Use Unique Passwords	●	●	●
5.3	Disable Dormant Accounts	●	●	●
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	●	●	●
5.5	Establish and Maintain an Inventory of Service Accounts		●	●
5.6	Centralize Account Management		●	●
06	**Access Control Management**			
6.1	Establish an Access Granting Process	●	●	●
6.2	Establish an Access Revoking Process	●	●	●
6.3	Require MFA for Externally-Exposed Applications	●	●	●
6.4	Require MFA for Remote Network Access	●	●	●
6.5	Require MFA for Administrative Access	●	●	●
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems		●	●
6.7	Centralize Access Control		●	●
6.8	Define and Maintain Role-Based Access Control			●

Number	Control/Safeguard	IG1	IG2	IG3
07	**Continuous Vulnerability Management**			
7.1	Establish and Maintain a Vulnerability Management Process	●	●	●
7.2	Establish and Maintain a Remediation Process	●	●	●
7.3	Perform Automated Operating System Patch Management	●	●	●
7.4	Perform Automated Application Patch Management	●	●	●
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets		●	●
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		●	●
7.7	Remediate Detected Vulnerabilities		●	●
08	**Audit Log Management**			
8.1	Establish and Maintain an Audit Log Management Process	●	●	●
8.2	Collect Audit Logs	●	●	●
8.3	Ensure Adequate Audit Log Storage	●	●	●
8.4	Standardize Time Synchronization		●	●
8.5	Collect Detailed Audit Logs		●	●
8.6	Collect DNS Query Audit Logs		●	●
8.7	Collect URL Request Audit Logs		●	●
8.8	Collect Command-Line Audit Logs		●	●
8.9	Centralize Audit Logs		●	●
8.10	Retain Audit Logs		●	●
8.11	Conduct Audit Log Reviews		●	●
8.12	Collect Service Provider Logs			●
09	**Email and Web Browser Protections**			
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	●	●	●
9.2	Use DNS Filtering Services	●	●	●
9.3	Maintain and Enforce Network-Based URL Filters		●	●
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		●	●
9.5	Implement DMARC		●	●
9.6	Block Unnecessary File Types		●	●
9.7	Deploy and Maintain Email Server Anti-Malware Protections			●

Number	Control/Safeguard	IG1	IG2	IG3
10	**Malware Defenses**			
10.1	Deploy and Maintain Anti-Malware Software	●	●	●
10.2	Configure Automatic Anti-Malware Signature Updates	●	●	●
10.3	Disable Autorun and Autoplay for Removable Media	●	●	●
10.4	Configure Automatic Anti-Malware Scanning of Removable Media		●	●
10.5	Enable Anti-Exploitation Features		●	●
10.6	Centrally Manage Anti-Malware Software		●	●
10.7	Use Behavior-Based Anti-Malware Software		●	●
11	**Data Recovery**			
11.1	Establish and Maintain a Data Recovery Process	●	●	●
11.2	Perform Automated Backups	●	●	●
11.3	Protect Recovery Data	●	●	●
11.4	Establish and Maintain an Isolated Instance of Recovery Data	●	●	●
11.5	Test Data Recovery		●	●
12	**Network Infrastructure Management**			
12.1	Ensure Network Infrastructure is Up-to-Date	●	●	●
12.2	Establish and Maintain a Secure Network Architecture		●	●
12.3	Securely Manage Network Infrastructure		●	●
12.4	Establish and Maintain Architecture Diagram(s)		●	●
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)		●	●
12.6	Use of Secure Network Management and Communication Protocols		●	●
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		●	●
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			●

Number	Control/Safeguard	IG1	IG2	IG3
13	**Network Monitoring and Defense**			
13.1	Centralize Security Event Alerting		●	●
13.2	Deploy a Host-Based Intrusion Detection Solution		●	●
13.3	Deploy a Network Intrusion Detection Solution		●	●
13.4	Perform Traffic Filtering Between Network Segments		●	●
13.5	Manage Access Control for Remote Assets		●	●
13.6	Collect Network Traffic Flow Logs		●	●
13.7	Deploy a Host-Based Intrusion Prevention Solution			●
13.8	Deploy a Network Intrusion Prevention Solution			●
13.9	Deploy Port-Level Access Control			●
13.10	Perform Application Layer Filtering			●
13.11	Tune Security Event Alerting Thresholds			●
14	**Security Awareness and Skills Training**			
14.1	Establish and Maintain a Security Awareness Program	●	●	●
14.2	Train Workforce Members to Recognize Social Engineering Attacks	●	●	●
14.3	Train Workforce Members on Authentication Best Practices	●	●	●
14.4	Train Workforce on Data Handling Best Practices	●	●	●
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	●	●	●
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	●	●	●
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	●	●	●
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	●	●	●
14.9	Conduct Role-Specific Security Awareness and Skills Training		●	●
15	**Service Provider Management**			
15.1	Establish and Maintain an Inventory of Service Providers	●	●	●
15.2	Establish and Maintain a Service Provider Management Policy		●	●
15.3	Classify Service Providers		●	●
15.4	Ensure Service Provider Contracts Include Security Requirements		●	●
15.5	Assess Service Providers			●
15.6	Monitor Service Providers			●
15.7	Securely Decommission Service Providers			●

Number	Control/Safeguard	IG1	IG2	IG3
16	**Application Software Security**			
16.1	Establish and Maintain a Secure Application Development Process		●	●
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		●	●
16.3	Perform Root Cause Analysis on Security Vulnerabilities		●	●
16.4	Establish and Manage an Inventory of Third-Party Software Components		●	●
16.5	Use Up-to-Date and Trusted Third-Party Software Components		●	●
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		●	●
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure		●	●
16.8	Separate Production and Non-Production Systems		●	●
16.9	Train Developers in Application Security Concepts and Secure Coding		●	●
16.10	Apply Secure Design Principles in Application Architectures		●	●
16.11	Leverage Vetted Modules or Services for Application Security Components		●	●
16.12	Implement Code-Level Security Checks			●
16.13	Conduct Application Penetration Testing			●
16.14	Conduct Threat Modeling			●
17	**Incident Response Management**			
17.1	Designate Personnel to Manage Incident Handling	●	●	●
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	●	●	●
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	●	●	●
17.4	Establish and Maintain an Incident Response Process		●	●
17.5	Assign Key Roles and Responsibilities		●	●
17.6	Define Mechanisms for Communicating During Incident Response		●	●
17.7	Conduct Routine Incident Response Exercises		●	●
17.8	Conduct Post-Incident Reviews		●	●
17.9	Establish and Maintain Security Incident Thresholds			●
18	**Penetration Testing**			
18.1	Establish and Maintain a Penetration Testing Program		●	●
18.2	Perform Periodic External Penetration Tests		●	●
18.3	Remediate Penetration Test Findings		●	●
18.4	Validate Security Measures			●
18.5	Perform Periodic Internal Penetration Tests			●