



**Little River Band of Ottawa Indians**  
2608 Government Center Drive  
Manistee, MI 49660  
(231) 723-8288

**Moved to  
Open Session  
02/03/21**

**Resolution # 20-0909-249**

*Acceptance of the Little River Band of Ottawa Indians 2020 Cyber Security Risk  
Assessment by Rehmann*

WHEREAS, the status of the *Gaá Čhing Ziibi Daáwaa Aníshinábek* (Little River Band of Ottawa Indians) as a sovereign and Treaty-making power is confirmed in numerous treaties, from agreements with the initial colonial powers on this land, to various treaties with the United States; and

WHEREAS, the Little River Band of Ottawa Indians (Tribe) is descended from, and is the political successor to, the Grand River Ottawa Bands, signatories of the 1836 Treaty of Washington (7 Stat. 491) with the United States, as reaffirmed by federal law in P.L. 103-324, enacted in 1994; and

WHEREAS, the Tribe adopted a new Constitution, pursuant to a vote of the membership on May 27, 1998, which Constitution became effective upon its approval by the Assistant Secretary-Indian Affairs on July 10, 1998; and

WHEREAS, the Tribe adopted amendments to the Constitution on April 26, 2004, which became effective upon approval by the Assistant Secretary-Indian Affairs on May 13, 2004; and

WHEREAS, the Tribe adopted amendments to the Constitution on July 11, 2016 which became effective upon approval by the Assistant Secretary-Indian Affairs on August 24, 2016; and

WHEREAS, the Tribal Council adopted, in accordance with Article IV, Section 7(a) of the Constitution and the Government Business and Accounting Act of 2010 which identifies how external audits are conducted and reported by the Tribe; and

WHEREAS, the Tribe conducts assessments and audits of its activities for the purpose of compliance with federal laws and agreements with external entities; and

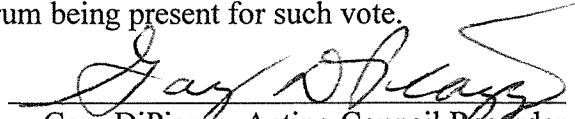
WHEREAS, the Tribe has caused to be conducted an Assessment of Little River Band of Ottawa Information Technology Cyber Security Risk as Report by Rehmann Robson dated July 7<sup>th</sup>, 2020; and


WHEREAS, Rehmann has presented the Cyber Security Risk Assessment finds in detail to Tribal Council and Ogema in a work session on Friday August 21<sup>st</sup> 2020;

NOW THEREFORE IT IS RESOLVED THAT the Tribal Council of the Little River Band of Ottawa Indians hereby accepts the Little River Band of Ottawa Indians Information Technology Risk Assessment dated July 7<sup>th</sup>, 2020.

**CERTIFICATE OF ADOPTION**

I do hereby certify that the foregoing resolution was duly presented and adopted by the Tribal Council with 8 FOR, 0 AGAINST, 0 ABSTAINING, and 1 ABSENT at a Regular Closed Session of the Little River Band of Ottawa Indians Tribal Council held on September 9th, 2020, via ZOOM, with a quorum being present for such vote.

  
Gary DiPiazza, Acting Council Recorder

  
Ron Pete, Acting Council Speaker

Attest:

Distribution: Council Records  
Tribal Ogema



## **Little River Band of Ottawa Indians**

2608 Government Center Drive

Manistee, MI 49660

(231) 723-8288

### **Resolution # 20-0909-249**

#### *Acceptance of the Little River Band of Ottawa Indians 2020 Cyber Security Risk Assessment by Rehmann*

WHEREAS, the status of the *Gaá Čhíng Ziibi Daáwaa Aníshinaábek* (Little River Band of Ottawa Indians) as a sovereign and Treaty-making power is confirmed in numerous treaties, from agreements with the initial colonial powers on this land, to various treaties with the United States; and

WHEREAS, the Little River Band of Ottawa Indians (Tribe) is descended from, and is the political successor to, the Grand River Ottawa Bands, signatories of the 1836 Treaty of Washington (7 Stat. 491) with the United States, as reaffirmed by federal law in P.L. 103-324, enacted in 1994; and

WHEREAS, the Tribe adopted a new Constitution, pursuant to a vote of the membership on May 27, 1998, which Constitution became effective upon its approval by the Assistant Secretary-Indian Affairs on July 10, 1998; and

WHEREAS, the Tribe adopted amendments to the Constitution on April 26, 2004, which became effective upon approval by the Assistant Secretary-Indian Affairs on May 13, 2004; and

WHEREAS, the Tribe adopted amendments to the Constitution on July 11, 2016 which became effective upon approval by the Assistant Secretary-Indian Affairs on August 24, 2016; and

WHEREAS, the Tribal Council adopted, in accordance with Article IV, Section 7(a) of the Constitution and the Government Business and Accounting Act of 2010 which identifies how external audits are conducted and reported by the Tribe; and

WHEREAS, the Tribe conducts assessments and audits of its activities for the purpose of compliance with federal laws and agreements with external entities; and

WHEREAS, the Tribe has caused to be conducted an Assessment of Little River Band of Ottawa Information Technology Cyber Security Risk as Report by Rehmann Robson dated July 7<sup>th</sup>, 2020; and

WHEREAS, Rehmann has presented the Cyber Security Risk Assessment finds in detail to Tribal Council and Ogema in a work session on Friday August 21<sup>st</sup> 2020;

NOW THEREFORE IT IS RESOLVED THAT the Tribal Council of the Little River Band of Ottawa Indians hereby accepts the Little River Band of Ottawa Indians Information Technology Risk Assessment dated July 7<sup>th</sup>, 2020.

**CERTIFICATE OF ADOPTION**

I do hereby certify that the foregoing resolution was duly presented and adopted by the Tribal Council with 8 FOR, 0 AGAINST, 0 ABSTAINING, and 1 ABSENT at a Regular Closed Session of the Little River Band of Ottawa Indians Tribal Council held on September 9th, 2020, via ZOOM, with a quorum being present for such vote.

---

Gary DiPiazza, Acting Council Recorder

---

Ron Pete, Acting Council Speaker

Attest:

Distribution:      Council Records  
                         Tribal Ogema

7/17/2020



# Delivering Business Wisdom

CYBER SECURITY RISK ASSESSMENT REPORT FOR

## Little River Band of Ottawa Indians

Submitted by:

Louis DeVito

Tim Weber

[louis.devito@rehmann.com](mailto:louis.devito@rehmann.com) | [tim.weber@rehmann.com](mailto:tim.weber@rehmann.com)

Rehmann | 3145 Prairie St. SW | Grandville, MI 49418 | 616.222-9200

Contains STATUS UPDATE AS OF JANUARY 26th. 2021.

---

## Table of Contents

<b>1. Cover Letter .....</b>	<b>1</b>
<b>2. Executive Summary .....</b>	<b>2</b>
High Priority Issues Identified .....	2
Moderate Priority Issues Identified .....	3
Low Priority Issues Identified .....	5
Comments Identified .....	5
Areas Reviewed Without Findings .....	5
<b>3. Identify .....</b>	<b>6</b>
3.01. NIST ID.GV-1   Governance .....	6
3.02. NIST ID.GV-3   Governance .....	6
3.03. NIST ID.AM-1   Asset Management .....	6
3.04. NIST ID.RM-1   Risk Management .....	7
3.05. NIST ID.RA-1   Risk Assessment .....	7
3.06. NIST ID.BE-5   Business Environment .....	7
<b>4. Protect .....</b>	<b>7</b>
4.01. NIST PR-IP-2   Information Protection .....	7
4.02. NIST PR-IP-9   Information Protection .....	8
4.03. NIST PR-AC-1   Identity Management .....	8
4.04. NIST PR-AC-4   Identity Management .....	8
4.05. NIST PR-AC-3   Identity Management .....	9
4.06. NIST PR-IP-1   Information Protection .....	9
4.07. NIST PR-AT-1   Awareness / Training .....	9
<b>5. Respond .....</b>	<b>10</b>
5.01. NIST RS-RP-1   Response Planning .....	10
<b>6. Miscellaneous .....</b>	<b>10</b>
6.01. Infrastructure .....	10
6.02. Administrator Account Use .....	11
6.03. Endpoint Security .....	11
6.04. Endpoint Security .....	11
6.05. Logging .....	12
6.06. Logging .....	12
6.07. Infrastructure .....	12
6.08. Infrastructure .....	13
6.09. Infrastructure .....	13

---

August 10, 2020

Audit Committee  
Little River Band of Ottawa Indians

,

Maintaining a strong internal control environment is an ongoing process that involves identifying, assessing and mitigating risks. During our visit, we were able to meet with management, review processes and policies currently in place, and through related procedures, identify instances that represent opportunities for management to improve upon your company's internal control structure.

We have performed the procedures listed in Executive Summary solely to assist the Audit Committee in fulfilling its oversight responsibilities relating to your company's information technology internal control process. The results of our procedures and any corresponding recommendations are also listed in the following report.

We have not performed, or been engaged to perform, any procedures beyond those procedures selected by management and the Audit Committee and which were outlined in the planned calendar of assistance. The sufficiency of the procedures is solely the responsibility of the Audit Committee. Because the procedures performed do not constitute an audit, examination, or review of your company's financial statements, we do not express an opinion on your financial statements or any elements, accounts, or items thereof, nor do we offer any assurance on your company's risk management system. Matters communicated in this report are those that existed as of the report date and cannot be projected to any future periods, as controls may deteriorate or other conditions that affect the risk management environment may change. Management responses to identified findings and related recommendations included in our report have not been subjected to our procedures.

Our comments and recommendations, all of which have been discussed with your appropriate company personnel, are intended to assist your company in improving the integrity, maintenance, and security of the institution. We will be pleased to discuss these comments in further detail at your convenience, perform an additional study of these matters, or assist you in implementing any of our recommendations.

Sincerely,

---

## 2. Executive Summary

Rehmann Robson performed an information technology audit and assessment consisting of the following:

Identify, Protect, Detect, Respond, Miscellaneous

We have quantified the results of our assessment as follows: A grade of satisfactory was applied if, overall the elements of the internal control structure provide reasonable assurance that the relevant risks to the institution's operating activities are effectively controlled and no risks were identified that require management's immediate attention or escalation. A grade of satisfactory with exceptions was assigned if overall the elements of the internal control structure provide reasonable assurance that the relevant risks to the institution's operating activities are effectively controlled; however, there were some control exceptions noted. A grade of unsatisfactory was applied if overall the elements of the internal control structure do not provide reasonable assurance that the relevant risks to the institution's operating activities are adequately controlled.

Based on the results of our procedures, we found the overall level of control to be *satisfactory with exceptions* for an institution of your size and complexity. Our overview of findings and comments are noted below.

To facilitate analysis of our recommendations, we have categorized our findings as high, moderate, or low priority. We have also included any relevant comments. These categories were assigned to each finding to assist management and the Audit Committee in prioritizing the recommendations. We encourage management and the Audit Committee to evaluate each recommendation and related priority independent of this report. The following is a summary of our findings and comments during this engagement. Our full report of procedures, comments, findings, and recommendations is attached.

### High Priority Issues Identified

"High Priority Issues" are issues that should be addressed immediately and corrective action taken to mitigate or reduce the risk, and ensure the underlying control is strengthened to prevent possible future deficiencies. This rating is assigned for one or more of the following reasons:

- A potentially severe security vulnerability is identified that could affect the confidentiality, integrity, or availability of the systems, applications, or data.
- Deficiency in a significant control area is identified that could place the confidentiality, integrity, or availability of the systems, applications, or data at risk.
- A control area required to be addressed by regulatory agencies that is either missing or does not address all the critical items.
- A moderate type finding from a previous report that has not been corrected.

*Three (3) high priority issues were identified. The following is a summary of those issues:*

- \* NIST PR-IP-2 | Information Protection - Implement a backup process that ensures that you have 3 copies of your data, on two different storage media, 1 of which is offsite and offline.
  - o Test your restores. A backup has zero value if it fails when trying to implement a restore. Testing is critical to identify any issues with the backup process, and to be confident that restores will be successful when needed.

\* COMPLETED.



\* NIST PR-IP-9 | Information Protection - Create a business continuity and disaster recovery plan. Train your staff on the plan, work through table top exercises, and ensure that your organization is appropriately prepared in the event that a serious incident impacts the business. Failure to take these actions has put many a company out of business.

\* Infrastructure - Ensure that support contracts are available and valid for all critical infrastructure. In the event of an outage, support will often need to be engaged to provide vendor support. If you have equipment out of support, it is much more likely that an incident involving said equipment will drag on longer, and prolong the duration of the outage. For some systems, the monetary value of being down can be significant, though this should be evaluated to identify the level of support that is required. Additionally, some vendors require valid support contracts to patch devices. Without those contracts, patching stops, and your equipment becomes more vulnerable as it falls farther behind.

### Moderate Priority Issues Identified

"Moderate Priority Issues" are issues that should be addressed promptly and tracked to ensure corrective action is taken within a reasonable time. The weakness does not typically, by itself, produce an immediate risk, but could affect the confidentiality, integrity, or availability of the systems, applications, or data in conjunction with other weaknesses or factors. This rating is assigned for one or more of the following reasons:

- Security vulnerability is identified that, based on best-practices or other industry information, poses a risk.
- Deficiency in a control area is identified that could place the confidentiality, integrity, or availability of the systems, applications, or data at risk.
- Exceptions were found in reviewing and evaluating a significant control.
- Control area required to be addressed by regulatory agencies that do not address all the significant items.

*Eighteen (19) moderate priority issues were identified. The following is a summary of those issues:*

- \* NIST ID.GV-1 | Governance - Develop an information security policy, which covers the high level goals. Include procedures which identify what will be done to maintain compliance with policy, and processes for specifically how those procedures will be accomplished.
  - Assign an executive with overall ownership of the security posture of the organization. Consider hiring a CISO. And assign specific management and technical tasks to staff.
- \* NIST ID.GV-3 | Governance - Identify and review regulatory requirements, and create a plan for maintaining compliance.
  - NIST ID.AM-1 | Asset Management - Implement an IT asset management system, so that you can track hardware, software, support, and licensing information.
  - NIST ID.RM-1 | Risk Management - Implement a risk management process, so that as new risks are identified, they're handled in a consistent manner. Without this in place, it is common for many risks to be ignored, which can sometimes have disastrous consequences.
  - NIST ID.RA-1 | Risk Assessment - Implement a patch management system such that all operating systems, applications, and infrastructure assets are patched on a regular basis.
  - NIST ID.BE-5 | Business Environment - Identify the cost to the business if critical systems become unavailable, and use that information to drive decisions about the correct level of resilience in your environment. Resilience includes the ability to withstand and recover from outages, attacks, threats, and incidents.

\* Completed!

⊙ GOAL MAY NOT BE FEASIBLE.

• NEED FURTHER DISCUSSION ON SOLUTION!

- ① NIST PR-AC-1 | Identity Management - Consider implementing a single identify management solution, that can be used across the environment, instead of having numerous individual accounts for each separate login.
- \* NIST PR-AC-4 | Identity Management - Least privilege reduces the risk and/or impact of attackers gaining access to systems or data. Review access rights for individuals and groups in the organization, and ensure that only rights which are necessary are granted.
- \* NIST PR-AC-3 | Identity Management - Monitor remote access to the environment, and review or alert on unusual activity.
  - Configure MFA for all public facing sensitive connections. It is extremely common for public facing access portals to get breached via password spraying or phishing attacks. MFA provides an extra layer of security that is difficult to bypass, and can help keep these services secure.
- ① NIST PR-IP-1 | Information Protection - Implement a change control board that all infrastructure and systems changes must be filtered through.
- \* NIST RS-RP-1 | Response Planning - Implement an incident response plan, that covers the entire incident response lifecycle. The lifecycle begins and preparation, and includes detection, analysis, containment, eradication, recovery, and finally moves to post-incident activity, before returning to the preparation phase.
  - Each incident is an opportunity to learn from what went well, and what could have been improved. Make sure to leverage the lessons learned from past events, to help make future events run more smoothly and/or less frequently.
- \* Administrator Account Use - Create unprivileged accounts for administrators to use during routine computer work. Privileged accounts should only ever be used for logging into secure systems, to perform administrative tasks. Separating these accounts goes a long way towards limiting the attack surface for malware or a bad actor.
  - Require your administrators to not simply use their privileged accounts all the time for everything. This limits the attack surface for malware or bad actors.
- \* Endpoint Security - Encrypting drives helps prevent loss of data in the event that devices get lost or stolen. Put a drive encryption system in place on all company devices.
- \* Endpoint Security - Implement a host based IPS system, to provide advanced endpoint protection, above and beyond what standard AV can provide.
- \* Logging - Put a centralized logging solution into place, so that there is a single place where logs are aggregated. This will greatly assist in troubleshooting and root cause analysis for a variety of issues.
  - Configure alerting for critical even logs, but take care to not over configure alerting, as alert fatigue can be nearly as big of a problem as not having enough alerting.
- \* Logging - Implement a data governance solution, so that it becomes possible to manage and monitor what is happening to your data.
- \* Infrastructure - Perform network hardening on all network infrastructure, including firewalls, switches, and routers. This helps protect sensitive information from leaking out of your environment.
- \* Infrastructure - Ensure that all core systems infrastructure is not end of life. Any devices or systems that are, need to be scheduled for a refresh at the latest, during the next budget cycle. Ideally during the current budget cycle, if possible. End of life systems typically stop receiving patches, may not be eligible for support, and are much more likely to exhibit issues, which can cause significant unplanned downtime.
- ① Infrastructure - Ensure that your environment is consistent. A mixed environment is more expensive to support, and can cause compatibility or capability issues. Standardize on one vendor and product family for each type of infrastructure. Ensure that operating systems are consistent across the environment, and decommission legacy operating systems. Ensure that endpoints are as consistent as possible, so that the fewest number of images can be used to support devices.

\* COMPLETED:

① GOAL MAY NOT BE FEASIBLE

---

### Low Priority Issues Identified

“Low Priority Issues” are issues that should be reviewed and may provide an opportunity to improve a security weakness or control weakness. This rating is assigned for one or more of the following reasons:

- Security configuration weakness is identified based on best-practices or other industry information.
- Exceptions were found in reviewing and evaluating a control.

*One (1) low priority issue was identified. Detailed information regarding the low priority issue is documented in the complete report.*

### Comments Identified

These are recommendations that represent a possible opportunity to improve a process, system, or security control. These items do not necessarily place any process or system at risk.

*No comments were identified.*

### Areas Reviewed Without Findings

*The following reviews did not identify any high, moderate, low, or comment findings:*

---

## 3. Identify

### 3.01. NIST ID.GV-1 | Governance

#### Procedure

Is an organizational information security policy in place?

#### Findings

An organizational information security policy is not in place.

- ♦ Information security roles and responsibilities are not clearly assigned throughout the organization.

#### Priority - Moderate

#### Recommendation

Develop an information security policy, which covers the high level goals. Include procedures which identify what will be done to maintain compliance with policy, and processes for specifically how those procedures will be accomplished.

- ♦ Assign an executive with overall ownership of the security posture of the organization. Consider hiring a CISO. And assign specific management and technical tasks to staff.

### 3.02. NIST ID.GV-3 | Governance

#### Procedure

Is there a process in place for maintaining compliance with legal and regulatory requirements?

#### Findings

There is not a process in place for maintaining compliance with legal and regulatory requirements.

#### Priority - Moderate

#### Recommendation

Identify and review regulatory requirements, and create a plan for maintaining compliance.

### 3.03. NIST ID.AM-1 | Asset Management

#### Procedure

Is an IT asset management system in place?

#### Findings

An IT asset management system is not in place.

#### Priority - Moderate

#### Recommendation

Implement an IT asset management system, so that you can track hardware, software, support, and licensing information.

---

### 3.04. NIST ID.RM-1 | Risk Management

#### **Procedure**

Is there a risk management process in place?

#### **Findings**

A risk management process is not in place.

#### **Priority - Moderate**

#### **Recommendation**

Implement a risk management process, so that as new risks are identified, they're handled in a consistent manner. Without this in place, it is common for many risks to be ignored, which can sometimes have disastrous consequences.

### 3.05. NIST ID.RA-1 | Risk Assessment

#### **Procedure**

Is a patch management process in place?

#### **Findings**

A patch management process is not in place.

#### **Priority - Moderate**

#### **Recommendation**

Implement a patch management system such that all operating systems, applications, and infrastructure assets are patched on a regular basis.

### 3.06. NIST ID.BE-5 | Business Environment

#### **Procedure**

Are your resilience requirements for all critical services clearly established?

#### **Findings**

Resilience requirements for all critical services are not yet clearly established.

#### **Priority - Moderate**

#### **Recommendation**

Identify the cost to the business if critical systems become unavailable, and use that information to drive decisions about the correct level of resilience in your environment. Resilience includes the ability to withstand and recover from outages, attacks, threats, and incidents.

## 4. Protect

### 4.01. NIST PR-IP-2 | Information Protection

#### **Procedure**

Does your backup policy follow best practices, and utilize the 321 principle?

---

## Findings

The backup policy does not follow best practices, and utilize the 321 principle.

- ♦ Backup restores are not tested regularly.

## Priority - High

## Recommendation

Implement a backup process that ensures that you have 3 copies of your data, on two different storage media, 1 of which is offsite and offline.

- ♦ Test your restores. A backup has zero value if it fails when trying to implement a restore. Testing is critical to identify any issues with the backup process, and to be confident that restores will be successful when needed.

## 4.02. NIST PR-IP-9 | Information Protection

### Procedure

Are response plans for business continuity and disaster recovery in place?

## Findings

Response plans for business continuity and disaster recovery are not in place.

## Priority - High

## Recommendation

Create a business continuity and disaster recover plan. Train your staff on the plan, work through table top exercises, and ensure that your organization is appropriately prepared in the event that a serious incident impacts the business. Failure to take these actions has put many a company out of business.

## 4.03. NIST PR-AC-1 | Identity Management

### Procedure

Is there an identity management solution in place?

## Findings

An identity management solution is not in place.

## Priority - Moderate

## Recommendation

Consider implementing a single identify management solution, that can be used across the environment, instead of having numerous individual accounts for each separate login.

## 4.04. NIST PR-AC-4 | Identity Management

### Procedure

Are access permissions granted using the principle of least privilege?

---

## Findings

Access permissions are not restricted using the principle of least privilege.

## Priority - Moderate

## Recommendation

Least privilege reduces the risk and/or impact of attackers gaining access to systems or data. Review access rights for individuals and groups in the organization, and ensure that only rights which are necessary are granted.

## 4.05. NIST PR-AC-3 | Identity Management

### Procedure

Is there a process in place for managing remote access into the environment?

## Findings

There is not a process in place for managing remote access into the environment.

- ♦ MFA is not configured for sensitive connections.

## Priority - Moderate

## Recommendation

Monitor remote access to the environment, and review or alert on unusual activity.

- ♦ Configure MFA for all public facing sensitive connections. It is extremely common for public facing access portals to get breached via password spraying or phishing attacks. MFA provides an extra layer of security that is difficult to bypass, and can help keep these services secure.

## 4.06. NIST PR-IP-1 | Information Protection

### Procedure

Is a change control process in place?

## Findings

A change control process is not in place.

## Priority - Moderate

## Recommendation

Implement a change control board that all infrastructure and systems changes must be filtered through.

## 4.07. NIST PR-AT-1 | Awareness / Training

### Procedure

Is an end user security awareness and training program in place?

## Findings

An end user security awareness and training program is not in place.

## Priority - Low

### Recommendation

Implement an end user awareness and training program. Email phishing training is critical. Also important is general internet security training, as well as providing training on your security policies and procedures.

## 5. Respond

### 5.01. NIST RS-RP-1 | Response Planning

#### Procedure

Is there an incident response plan in place?

#### Findings

There is not an incident response plan in place.

- ♦ The incident response plan does not incorporate lessons learned.

## Priority - Moderate

### Recommendation

Implement an incident response plan, that covers the entire incident response lifecycle. The lifecycle begins and preparation, and includes detection, analysis, containment, eradication, recovery, and finally moves to post-incident activity, before returning to the preparation phase.

- ♦ Each incident is an opportunity to learn from what went well, and what could have been improved. Make sure to leverage the lessons learned from past events, to help make future events run more smoothly and/or less frequently.

## 6. Miscellaneous

### 6.01. Infrastructure

#### Procedure

Are all network and systems infrastructure covered by current support contracts?

#### Findings

Not all network and systems infrastructure are covered by current support contracts.

## Priority - High

### Recommendation

Ensure that support contracts are available and valid for all critical infrastructure. In the even of an outage, support will often need to be engaged to provide vendor support. If you have equipment out of support, it is much more likely that an incident involving said equipment will drag on longer, and prolong the duration of the outage. For some systems, the monetary value of being down can be significant, though this should be evaluated to identify the level of support that is required. Additionally, some



---

vendors require valid support contracts to patch devices. Without those contracts, patching stops, and your equipment becomes more vulnerable as it falls farther behind.

## 6.02. Administrator Account Use

### Procedure

Do systems administrators have separate privileged and unprivileged accounts?

### Findings

Systems administrators do not have separate privileged and unprivileged accounts.

- ♦ There is not a policy in place restricting privileged accounts from logging into unprivileged devices.

### Priority - Moderate

### Recommendation

Create unprivileged accounts for administrators to use during routine computer work. Privileged accounts should only ever be used for logging into secure systems, to perform administrative tasks. Separating these accounts goes a long way towards limiting the attack surface for malware or a bad actor.

- ♦ Require your administrators to not simply use their privileged accounts all the time for everything. This limits the attack surface for malware or bad actors.

## 6.03. Endpoint Security

### Procedure

Is a hard drive encryption system in place on all devices across the organization?

### Findings

A hard drive encryption system is not in place on all devices across the organization.

### Priority - Moderate

### Recommendation

Encrypting drives helps prevent loss of data in the event that devices get lost or stolen. Put a drive encryption system in place on all company devices.

## 6.04. Endpoint Security

### Procedure

Is a host intrusion prevention system (IPS) in place across the organization?

### Findings

A host intrusion prevention system (IPS) is not in place across the organization.

### Priority - Moderate

---

### **Recommendation**

Implement a host based IPS system, to provide advanced endpoint protection, above and beyond what standard AV can provide.

### 6.05. Logging

#### **Procedure**

Are device logs collected by a single, centralized tool?

#### **Findings**

Device logs are not collected by a single, centralized tool.

- ♦ That tool does not allow for detailed reporting or alerting on data.

#### **Priority - Moderate**

#### **Recommendation**

Put a centralized logging solution into place, so that there is a single place where logs are aggregated. This will greatly assist in troubleshooting and root cause analysis for a variety of issues.

- ♦ Configure alerting for critical even logs, but take care to not over configure alerting, as alert fatigue can be nearly as big of a problem as not having enough alerting.

### 6.06. Logging

#### **Procedure**

Is there a data governance solution in place?

#### **Findings**

A data governance solution is not in place.

#### **Priority - Moderate**

#### **Recommendation**

Implement a data governance solution, so that it becomes possible to manage and monitor what is happening to your data.

### 6.07. Infrastructure

#### **Procedure**

Has the network been hardened to ensure best practices are in place?

#### **Findings**

The network has not been hardened to ensure best practices are in place.

#### **Priority - Moderate**

#### **Recommendation**

Perform network hardening on all network infrastructure, including firewalls, switches, and routers. This helps protect sensitive information from leaking out of your environment.

---

## 6.08. Infrastructure

### Procedure

Are all network and systems infrastructure current, and not end of life?

### Findings

Not all network and systems infrastructure are current, and not end of life.

### Priority - Moderate

### Recommendation

Ensure that all core systems infrastructure is not end of life. Any devices or systems that are, need to be scheduled for a refresh at the latest, during the next budget cycle. Ideally during the current budget cycle, if possible. End of life systems typically stop receiving patches, may not be eligible for support, and are much more likely to exhibit issues, which can cause significant unplanned downtime.

## 6.09. Infrastructure

### Procedure

Is the network and systems infrastructure consistent, and not a mixed environment?

### Findings

The network and systems infrastructure is currently a mixed environment.

### Priority - Moderate

### Recommendation

Ensure that your environment is consistent. A mixed environment is more expensive to support, and can cause compatibility or capability issues. Standardize on one vendor and product family for each type of infrastructure. Ensure that operating systems are consistent across the environment, and decommission legacy operating systems. Ensure that endpoints are as consistent as possible, so that the fewest number of images can be used to support devices.



LITTLE RIVER BAND of OTAWA INDIANS  
2608 Government Center Drive  
Manistee Michigan 49660

Information Technology Department

To: Tim Weber  
Louis DeVito

Copy: Aneudy Mota  
Andrew Jeurink

Date: July 29, 2020

RE: Cyber Security Assessment Report for Little River Band of Ottawa Indians.  
Submitted by Louis DeVito and Tim Weber dated 7/17/20. (H.A. the report).

I have reviewed the report submitted and found that many of the "findings" in the report are based on incorrect information.

Some of the "findings" and recommendations are not feasible for the size of the IT Department. The rural nature of the Tribal Government locations makes it difficult to acquire staff and to retain them. Some items commonly identified as best practices within the IT Industry and some businesses, simply cannot be applied as the cost and complexity is beyond the means and ability of the Tribal Government.

Further many of the "findings" are what the IT Director considers as Out of Scope. Those out of scope items are outside the ability of the IT Department to impact.

The Report States:

- "NIST PR-IP-2 | Information Protection - Implement a backup process that ensures that you have 3 copies of your data, on two different storage media, 1 of which is offsite and offline. Test your restores. A backup has zero value if it fails when trying to implement a restore. Testing is critical to identify any issues with the backup process, and to be confident that restores will be successful when needed.

Response:

The Tribal Government has backups, in the form of disk drives, in multiple locations, with another set of backups residing in the cloud. In section 4.01 the report refers to the 321 principle of backup. A principle developed and based on tape technology. Obviously, tape technology is inadequate for the size of our current data storage requirements (203TB). Even the latest tape generation would be costly to implement, costly to maintain and costly to operate, and require a large amount of man hours for tape handling.

As the Tribal Government moves forward with the cloud implementation a different principle is planned using geo-replication. Three copies of the data; One is production based in cloud servers; Two a replication of data on a different cloud service; Three an offline copy created daily in batch on a third cloud service.

Test the ability to restore ... not only is this completed weekly, the current backup system was used to completely restore the entire network during the week of March 9, 2020. Also, the restore capability was used multiple times during the last month. Testing the ability to restore becomes a moot point when files are restored as part of routine IT activity.

The Report States:

NIST PR-IP-9 | Information Protection - Create a business continuity and disaster recover plan. Train your staff on the plan, work through table top exercises, and ensure that your organization is appropriately prepared in the event that a serious incident impacts the business. Failure to take these actions has put many a company out of business.

Response:

This out of scope. The IT Department cannot create this plan. This work must be completed at a higher leadership level. The IT Department simply does not have the authority to require other program directors to work with IT on creating such a plan. The IT Director can only work within the confines of Information Technology and have a plan in place to replace equipment and restore data in the case of disaster. These plans are in place as is the ability to restore data as discussed above.

The Report States:

Infrastructure - Ensure that support contracts are available and valid for all critical infrastructure. In the even of an outage, support will often need to be engaged to provide vendor support. If you have equipment out of support, it is much more likely that an incident involving said equipment will drag on longer, and prolong the duration of the outage. For some systems, the monetary value of being down can be significant, though this should be evaluated to identify the level of support that is required. Additionally, some vendors require valid support contracts to patch devices. Without those contracts, patching stops, and your equipment becomes more vulnerable as it falls farther behind.

Response:

All current hardware has maintenance available. Hardware is purchased with extended warranty (5 years) with NBD response. Server and storage hardware is replaced within 12 months of the manufactures end of life.

NOTE: hardware replacement is a function of the budgetary resources and current directives from Tribal Government Leadership has been to cut all program budgets. Currently there is not sufficient budgetary resources to replace equipment in budget year 2020 or budget year 2021. IT cannot replace end of life equipment with out the resources to do so.

The Report States:

NIST ID.GV-1 | Governance - Develop an information security policy, which covers the high level goals. Include procedures which identify what will be done to maintain compliance with policy, and processes for specifically how those procedures will be accomplished.  
Assign an executive with overall ownership of the security posture of the organization. Consider hiring a CISO. And assign specific management and technical tasks to staff.

Response:

An information security plan was developed and approved in 2013.  
IT-2050 Information Security Policy.

The recommendation to "assign an Executive" is out of scope. The IT Department cannot assign an executive. Currently by job description and at the direction of the Tribal Ogema the IT Director is the HIPAA Security Officer as defined in 45 CFR 164.530 (ii). Currently by job description and by the direction of the Tribal Ogema the IT Director is the LASO (Local Agency Security Officer) as defined in FBI Criminal Justice Security Policy (document CJIS-ITS-DOC-08140-5.9) Section 3.2.2.2.e.

The Report States:

NIST ID.GV-3 | Governance - Identify and review regulatory requirements, and create a plan for maintaining compliance.

Response:

The Tribal Government has a Unified Legal Department that works closely with the IT Director. The IT Director routinely reviews appropriate regulation as directed in PHI Policy manual section 3.3 Workforce Training. Also, in the CJIS Policy Manual section 5.2.2 requiring annual training for the designated LASO.

The Report States:

NIST ID.AM-1 | Asset Management - Implement an IT asset management system, so that you can track hardware, software, support, and licensing information.

NIST PR-AC-3 | Identity Management - Monitor remote access to the environment, and review or alert on unusual activity.

Configure MFA for all public facing sensitive connections. It is extremely common for public facing access portals to get breached via password spraying or phishing attacks. MFA provides an extra layer of security that is difficult to bypass, and can help keep these services secure.

Logging - Put a centralized logging solution into place, so that there is a single place where logs are aggregated. This will greatly assist in troubleshooting and root cause analysis for a variety of issues.

Configure alerting for critical even logs, but take care to not over configure alerting, as alert fatigue can be nearly as big of a problem as not having enough alerting.

Logging - Implement a data governance solution, so that it becomes possible to manage and monitor what is happening to your data.

Response:

The Tribal Government IT Department does in fact have an asset management system. The IT Department uses a complete monitor, logging, and error tracking system along with help desk and asset management and control. This system is from Solar Winds and comprises the Orion Package, and the Dameware Package.

The Report States:

Endpoint Security - Encrypting drives helps prevent loss of data in the event that devices get lost or stolen. Put a drive encryption system in place on all company devices.

Endpoint Security - Implement a host based IPS system, to provide advanced endpoint protection, above and beyond what standard AV can provide.

Response:

The Tribal Government currently utilizes SOPHOS End Point Security; SOPHOS EMAIL Security; SOPHOS Internet Security. All portable devices are secured with drive encryption (Bitlocker) and separate passwords.

The Report States:

- NIST ID.RM-1 | Risk Management - Implement a risk management process, so that as new risks are identified, they're handled in a consistent manner. Without this in place, it is common for many risks to be ignored, which can sometimes have disastrous consequences.

Response:

In accordance with PHI Policy Manual Section 5.1 a risk assessment is completed and reviewed annually as required by 45 CFR 164.308 (a)1 (ii)(A)

The Report States:

NIST ID.RA-1 | Risk Assessment - Implement a patch management system such that all operating systems, applications, and infrastructure assets are patched on a regular basis.

Response:

IT Director concurs with this, a patch management system would be welcome addition to the IT Department. That said the matter of who will maintain the system and actually complete the patching of systems and hardware needs to be addressed. Currently all six IT Employees perform the functions of two positions. Microsoft software updates and upgrades are applied two weeks after release. Firmware updates are completed as soon as possible, dependent upon staff availability.

#### The Report States:

- NIST ID.BE-5 | Business Environment - Identify the cost to the business if critical systems become unavailable, and use that information to drive decisions about the correct level of resilience in your environment. Resilience includes the ability to withstand and recover from outages, attacks, threats, and incidents.

NIST PR-AC-1 | Identity Management - Consider implementing a single identify management solution, that can be used across the environment, instead of having numerous individual accounts for each separate login.

#### Response:

This is out of the scope of the IT Department. Each individual department/program chooses their own software to operate with. IT has no say in the decision other than can the software operate on the Tribal Government network. Thus, the network consists of multiple LINUX and Windows based systems. All systems in use by the individual programs are supported the software vendor and under the control of the individual programs. For Example: The Tribal Court uses Justware and the Court Administrator is the Justware Administrator. The Accounting Program uses MIP Fund Accounting. The CFO is the MIP Fund Accounting Administrator. Each individual program administers their own software and sets the rules on how they are used and by whom. A single identity system is not feasible.

#### The Report States:

NIST PR-AC-4 | Identity Management - Least privilege reduces the risk and/or impact of attackers gaining access to systems or data. Review access rights for individuals and groups in the organization, and ensure that only rights which are necessary are granted.

#### Response:

The IT Department controls the network USERID and LOGIN and sets the policy for network USERID creation and passwords. All of this is covered by:

IT-0050 – Acceptable Use Policy

IT-0100 – Network Password Policy

IT-1100 – Network and Application Access Policy

#### The Report States:

- NIST PR-IP-1 | Information Protection - Implement a change control board that all infrastructure and systems changes must be filtered through.

#### Response:

This outside the scope of the IT Department for application software. For network infrastructure this change is controlled by hardware replacement and network technology. A “change control board” is, in my opinion not feasible for the Tribal Government.



The Report States:

NIST RS-RP-1 | Response Planning - Implement an incident response plan, that covers the entire incident response lifecycle. The lifecycle begins and preparation, and includes detection, analysis, containment, eradication, recovery, and finally moves to post-incident activity, before returning to the preparation phase.

Each incident is an opportunity to learn from what went well, and what could have been improved. Make sure to leverage the lessons learned from past events, to help make future events run more smoothly and/or less frequently.

Response:

This is covered in IT-1200 – Security Incident Policy. Which is required by the PHI Policy Manual Section 5.7 and as required by 45 CFR 164.308 (a)(6).

The Report States:

Administrator Account Use - Create unprivileged accounts for administrators to use during routine computer work. Privileged accounts should only ever be used for logging into secure systems, to perform administrative tasks. Separating these accounts goes a long way towards limiting the attack surface for malware or a bad actor.

Require your administrators to not simply use their privileged accounts all the time for everything. This limits the attack surface for malware or bad actors.

Response:

The IT Director concurs with this statement. This will be implemented ASAP in by IT Directive.

The report states:

Infrastructure - Ensure that all core systems infrastructure is not end of life. Any devices or systems that are, need to be scheduled for a refresh at the latest, during the next budget cycle. Ideally during the current budget cycle, if possible. End of life systems typically stop receiving patches, may not be eligible for support, and are much more likely to exhibit issues, which can cause significant unplanned downtime.

Infrastructure - Ensure that your environment is consistent. A mixed environment is more expensive to support, and can cause compatibility or capability issues. Standardize on one vendor and product family for each type of infrastructure. Ensure that operating systems are consistent across the environment, and decommission legacy operating systems. Ensure that endpoints are as consistent as possible, so that the fewest number of images can be used to support devices

Response:

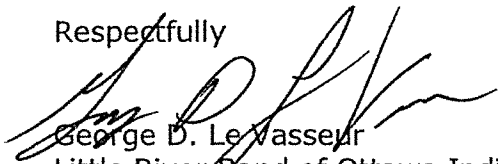
IT Director concurs with this policy and best practice. Every attempt is made to keep critical hardware and software updates it is not always possible. Critical hardware replacement is conditioned by available funding. Non-Microsoft software is controlled by individual programs. It is up to the individual programs to ensure they maintain their software.

A mixed environment is necessary for the Tribal Government because of the practice of individual programs selecting their own software. Some software requires an older operating system because the vendor has not updated, or the software is not capable of being updated.

Attachments:

- a. IT-2050 - Information Security Policy
- b. IT-0050 - Acceptable Use Policy
- c. IT-0100 - Network Password Policy
- d. IT-1100 - Network and Application Access Policy
- e. IT-1200 - Security Incident Policy

Respectfully

A handwritten signature in black ink, appearing to read 'George D. Le Vasseur', is written over the printed name.

George D. Le Vasseur  
Little River Band of Ottawa Indians Tribal Government  
Information Technology Director  
HIPAA Security  
LASO



**Little River Band of Ottawa Indians**  
Information Technology  
Policy and Procedure Manual

Signature of Approval
<i>Jay B. Rommel</i>
Tribal Ogema
Date 1/27/13

**IT-2050**  
**Information Security Policy**

**Purpose**

The Information Security Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative security of information that should not be disclosed inside and / or outside of Little River Band of Ottawa Indians (LRBOI) without proper authorization. The information covered in the Information Security Policy includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing). All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the security level definitions were created as guidelines and to emphasize common sense steps that you can take to protect LRBOI Confidential information (e.g., LRBOI Confidential information should not be left unattended in conference rooms).

*Please Note: The impact of these guidelines on daily activity should be minimal.*

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the Information Technology Director Little River Band of Ottawa Indians.

**Policy:**

**1.0 Scope**

All LRBOI information is categorized into two main classifications:

- LRBOI Public
- LRBOI Confidential

LRBOI Public information is information that has been declared public knowledge by the Speaker of Tribal Council, the Tribal Ogema, or the Chief Judge, and can freely be given to anyone without any possible damage to LRBOI.

LRBOI Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of the Tribe. Also included in LRBOI Confidential is information that is less critical, such as telephone directories, general Tribal information, personnel information, etc., which does not require as stringent a degree of protection. Included within LRBOI Confidential information is that information which is extremely sensitive, such as enrollment information, or any other information that can personally identify a Tribal Citizen or employee, access to this information is restricted to individuals specifically authorized by Ordinance, Regulation, Resolution or Government Policy.

A subset of LRBOI Confidential information is "LRBOI Third Party Confidential" information. This is confidential information belonging or pertaining to another entity which has been entrusted to LRBOI by that entity under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges



## Little River Band of Ottawa Indians

### Information Technology Policy and Procedure Manual

from extremely sensitive to information about the fact that we've connected a supplier / vendor into LRBOI's network to support our operations.

LRBOI personnel are encouraged to use common sense judgment in securing LRBOI Confidential information to the proper extent. If an employee is uncertain of the Security of a particular piece of information, he/she should contact their manager

## 2.0 Policy

The Security Guidelines below provide details on how to protect information at varying security levels. Use these guidelines as a reference only, as LRBOI Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the LRBOI Confidential information in question. This policy is in compliance with Tribal Council Resolution #08-0416-106.

### 2.1 Minimal Security:

- General LRBOI information; some personnel and technical information.
- Access: LRBOI employees, contractors, people with a business need to know.
- Distribution within LRBOI: Standard interoffice mail; approved electronic mail and electronic file transmission methods.
- Distribution outside of LRBOI internal mail: U.S. mail and other public or private carriers; approved electronic mail and electronic file transmission methods.
- Electronic distribution: No restrictions except that it is sent to only approved recipients.
- Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
- Disposal/Destruction: Shred outdated paper information in shredder on LRBOI premises; electronic data should be expunged and, or cleared. Reliably erase or physically destroy media.

**Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Marking guidelines for information in hardcopy or electronic form:

*Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "LRBOI Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "LRBOI Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, LRBOI information is presumed to be "LRBOI Confidential" unless expressly determined to be LRBOI Public information by a LRBOI employee with authority to do so.*

### 2.2 More Sensitive:

- Business, financial, technical, and most personnel information.
- Access: LRBOI employees and non-employees with signed non-disclosure agreements who have a business need to know.
- Distribution within LRBOI: Standard interoffice mail approved electronic mail and electronic file transmission methods.



## Little River Band of Ottawa Indians

### Information Technology Policy and Procedure Manual

- Distribution outside of LRBOI internal mail: Sent via U.S. mail or approved private carriers.
- Electronic distribution: No restrictions to approved recipients within <Company Name>, but should be encrypted or sent via a private link to approved recipients outside of LRBOI premises.
- Storage: Individual access controls are highly recommended for electronic information.
- Disposal/Destruction: Shred in shredder on LRBOI premises; electronic data should be expunged / cleared. Reliably erase or physically destroy media.

**Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Marking guidelines for information in hardcopy or electronic form:

*Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the Security level of the information increases, you may, in addition or instead of marking the information "LRBOI Confidential" or "LRBOI Proprietary", wish to label the information "LRBOI Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.*

### 2.3 Most Sensitive:

- Trade secrets & marketing, operational, personnel, financial, source code, & technical information, enrollment information, or any other information that can personally identify a Tribal Citizen or employee, other information integral to the success of the Tribe.
- Access: Only those individuals (LRBOI employees and non-employees) designated with approved access and signed non-disclosure agreements.
- Distribution within LRBOI: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
- Distribution outside of LRBOI internal mail: Delivered direct; signature required; approved private carriers.
- Electronic distribution: No restriction to approved recipients within LRBOI but it is highly recommended that all information be strongly encrypted.
- Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
- Disposal/Destruction: Strongly Encouraged: Shred in shredder on LRBOI premises; electronic data should be expunged / cleared. Reliably erase or physically destroy media.

**Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Marking guidelines for information in hardcopy or electronic form:

*Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that LRBOI Confidential information is very sensitive, you may should label the information "LRBOI Internal: Registered and Restricted", "LRBOI Eyes Only", "LRBOI Confidential" or similar labels at the discretion of your individual business unit or*



## **Little River Band of Ottawa Indians**

### **Information Technology Policy and Procedure Manual**

*department. Once again, this type of LRBOI Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.*

### **3.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and possible civil and/or criminal prosecution to the full extent of the law.

### **4.0 Definitions:**

#### **Appropriate measures**

To minimize risk to LRBOI from an outside business connection, LRBOI computers may only be used by authorized personnel, employees and elected and appointed officials. All access from outside the Tribal Government domain must be restricted. Only those elected officials, employees, and third parties authorized by the Information Technology Director will be granted external access.

#### **Configuration of LRBOI to-other business connections**

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary. All LRBOI to other business connections must be authorized by the Information Technology Director.

#### **Delivered Direct; Signature Required**

Do not leave in interoffice mail slot call the mail room for special pick-up of mail.

#### **Approved Electronic File Transmission Methods**

Includes supported FTP clients and Web browsers.

#### **Envelopes Stamped Confidential**

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

#### **Approved Electronic Mail**

Includes all email systems supported by the Information Technology Department. These include, but are not necessarily limited to, LRBOI-MAIL. If you have a business need to use other mailers contact the Information Technology Department. Use of email services other than LRBOI-MAIL requires the express written permission of the Information Technology Director.

#### **Approved Encrypted email and files**

All email and file attachments are to be encrypted via an SSL Certification currently in use by the LRBOI-MAIL server.

#### **LRBOI Information System Resources**

LRBOI Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.



## **Little River Band of Ottawa Indians**

### **Information Technology Policy and Procedure Manual**

#### **Expunge**

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data. Please contact the Information Technology Department if you have concerns about confidential or sensitive data on local computer drives.

#### **Individual Access Controls**

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. LRBOI uses unique USERID and passwords controlled by policy IT-0100-Network Password Policy.

#### **Insecure Internet Links**

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of LRBOI.

#### **Encryption**

Prior to transmitting confidential and/or sensitive information electronically the information must be secured in accordance with instructions from the Information Technology Department.

#### **One Time and Visitor Authentication**

One Time and Visitor Authentication for an Internet connection is accomplished by using a defined proxy USERID and password to connect to LRBOI's Internet provider. Contact the Information Technology Department to have this set up for any visitor.

#### **Physical Security**

- A. Documents. All physical documents containing any confidential or sensitive information must be kept in locked files when not in use. The higher the sensitivity of the document the more control that is needed.
- B. Electronic files. All electronic files must be stored on the LRBOI storage network (SAN). The physical security of desktop computers is difficult to maintain in the LRBOI environment and keeping confidential and/or sensitive information on internal local drives is not authorized. The only exception is the Enrolment database maintained on the Enrollment Director desktop.
- C. Electronic files on portable/mobile computers. Copying and storing confidential and/or sensitive information to any mobile computer (either a laptop or a PDA) is not recommended. However when necessary remember to never leave the device alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you.

#### **Private Link**

A Private Link is an electronic communications path that LRBOI has control over the entire distance of the link. For example, all LRBOI networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. A VPN connection via the internet is a private link.



**Little River Band of Ottawa Indians**  
Information Technology  
**Policy and Procedure Manual**

**Authority:**

As authorized in IT-0000 and by the signature of the Tribal Ogema on page one.

Review/Change	Date	Description	Initial
Change	10 Jan 13	Add change/review table updated format.	ADJ





**Little River Band of Ottawa Indians**  
Information Technology  
Policy and Procedure Manual

Signature of Approval

*Joseph B. Romelle*  
Tribal Ogema Date 6/20/17

**IT-0050 Acceptable use of Tribal Government  
Computers, communications services and network systems.**

**Purpose:**

Describe the Tribal Government policy on the use of Tribal Government computers, computer systems and software, communications services and network assets and systems.

**Policy:**

Employees are provided the use of a computer and access to the Tribe's network, email and communication systems for the execution of Tribal Business. Employees are expected to use the Tribal Government's computers, email and communications equipment and network assets for work-related activities only. Any personal use of the Tribal Government's computers and communications equipment and network assets should be kept to an absolute minimum and occur only during the employees non work hours.

Inappropriate use of the Tribal Government's computers, email and communications equipment and network assets includes, but is not limited to, any use that interferes with the employee's and/or co-worker's work performance or that violates any tribal policies, tribal, state, or federal laws.

The following examples of inappropriate use of the Tribal Government's computers, email and communications equipment and network assets apply during both work hours and non-work hours and includes, but are not limited to:

- Transmitting or receiving sexually explicit videos, images or comments;
- Transmitting or receiving materials, videos, images or comments that may offend or harass someone based on their race, color, sex, religion, national origin, age, veteran status, marital status, sexual orientation, or physical or mental disability;
- Using the Tribal Government email system for nongovernmental email;
- Using personal or internet email services for Tribal Government business;
- Using internet radio or video or other streaming media for non-work related activities;
- Using computers for personal profit-making purposes;
- Accessing and/or sharing tribal files, materials or data without proper authorization;
- Downloading, copying, installing or using unlicensed software;
- Disruptive acts, such as introducing viruses, spyware, adware or malware into the computer system;
- Using someone else's password or providing others with your password;

***All computers, email and communications equipment and network assets, all messages, data files and information stored therein, remain the property of the Tribal Government and under the control, custody, and supervision of the tribe. Employees have no expectation of privacy in their use of tribal computers and the tribe reserves the right to monitor all computer, network, and email and communications activity by employees.***



## Little River Band of Ottawa Indians

### Information Technology Policy and Procedure Manual

Only licensed software will be installed on Tribal computers. IT Department employees are the only employees authorized to install software on Tribal owned computers. The Director of the department in which the computer is assigned must authorize all software to be installed on Tribal computers and must ensure that the software is properly licensed. Employees issued laptop computers may be authorized to install software on their issued laptop if requested by the Department Director and approved by the IT Director.

#### **Internet:**

Employees are granted access to the Internet via the Tribal Government network communications systems for use in conducting Tribal Business only. Personal use of the internet is not authorized during normal work hours.

***All internet use and activity conducted via the Tribal Governments network communication system is monitored, logged and recorded, including use during non-work hours. Employees have no expectation of privacy when accessing the internet via the Tribal Government network communications system, including internet use during non-work hours. The Tribal Government reserves the right to block any and all internet traffic or activity as it sees fit to block.***

Employees will not initialize setup or otherwise create accounts in any on-line service without the written approval of their Department Director and the IT Director. Employee's so authorized shall disclose all passwords to the Tribe and their Director or the IT Director when requested but should not share the passwords with other employees. Employees' use of on-line service accounts shall be limited to work-related activities only.

Only IT Department employees are authorized to download software from the Internet.

Employees shall not duplicate or download from the Internet or from e-mail any materials (such as documents, photographs, and music and video files) that are copyrighted, patented, trademarked, or otherwise identified as intellectual property without express written permission from the owner of the material. When appropriate Internet material or e-mail files are downloaded, they should be scanned using the Tribal Government's antivirus software.

Employees who violate this policy are subject to disciplinary action up to, and including, termination of employment.

#### **Authority:**

As authorized in IT-0000 and by the signature of the Tribal Ogema on page one.

Review/Change	Date	Description	Initial
Change	5DEC12	Add annual review table	<i>DOJ</i>
Review	6JAN16	Minor wording changes and clarification	<i>DOJ</i>
Change	19FEB16	Prohibit the use of nongovernment email for government work.	<i>DOJ</i>
Review	08MAY17	Annual Review	<i>DOJ</i>



**Little River Band of Ottawa Indians**  
Information Technology  
Policy and Procedure Manual

Signature of Approval	
<i>Jerry D. Runkle</i>	
Tribal Ogema	Date
	6-2017

**IT- 0100**  
**NETWORK PASSWORD POLICY**

**Purpose:**

This policy establishes the criteria to be followed by all Authorized Users of Little River Band of Ottawa Indians (LRBOI) computers and network resources when creating an LRBOI Network password.

**Policy:**

Employees are required to create a new password the first time they login after IT sets or resets their password. All passwords have a lifespan of sixty days. When nearing the end of this sixty-day limit, you will be reminded that your password will soon expire and be prompted with the option to change your password. You should make the change at this time and not wait for the final expiration. After sixty days this change will be mandatory. However, at any time you may change your password as long as your previous password has aged at least one day (Note: The age limitation can be overridden by contacting IT if need be).

Passwords must remain confidential. Posting your password in your office or giving your password to anyone except your supervisor, director, or an IT Department employee is expressly prohibited. Please refer to IT-0050 Use of LRBOI Computers and Network for further details on password confidentiality.

The following are password security requirements:

All passwords are composed of the following non-optional conditions:

- A. Must be ten or more characters in length
- B. Must contain at least one numerical character 0 1 2 3 4 5 6 7 8 9
- C. Must contain at least one UPPER CASE alpha character.
- D. Must contain at least one special character i.e. ! @ # \$ % ^ & \* ( )
- E. Cannot be repeated or be similar to the last 20 passwords you have used.

Passwords may not contain:

- A. Repeated or sequential letters or numbers i.e. ABC or 123 or EEE or 7777.
- B. Dates or similarly formatted number sequences.

The following are guidelines for good password security:

Passwords could be created by:

- A. Substituting the number 0 for the letter O.
- B. Substituting the number 1 or special character ! for the letter I.
- C. Substituting the number 3 for the letter E.
- D. Substituting the special character @ for the letter A.
- E. Substituting the special character % for the letters R or T.

Similar substitutions can be used throughout the password the more random the better.



## Little River Band of Ottawa Indians

### Information Technology Policy and Procedure Manual

Passwords should not be:

- A. Easily identifiable words or phrases.
- B. Family or pet names.
- C. Foreign words or names.
- D. Written down and placed in an accessible spot.

*(You may write down your password but treat that piece of paper as if it were a credit card.)*

Passwords should be hard to guess; therefore a good password is a random sequence of letters (upper and lower case), numbers, and special characters. The best passwords have no meaning or significance to the creator and the very best passwords have no meaning what so ever.

The more unique and random you can make your password the better.

**Remember that you are responsible for all computer activity conducted by your USERID, so protect your password.**

#### **Automatic logout:**

Your network USERID Account will be automatically locked out if you fail to correctly enter your password 5 times with in a 15 minute time frame. Once locked out you must contact the IT Help Desk to get your account unlocked.

#### **Authority:**

As authorized in IT-0000 and by the signature of the Tribal Ogema on page one.

Review/Change	Date	Description	Initial
Change	12/5/12	Add annual review table log and change password length to 10 characters.	ADP
Change	7/27/15	Added automatic logout after 5 failed attempts within 15 minutes	ADP
Review	5/8/17	Annual Review	ADP



**Little River Band of Ottawa Indians**  
Information Technology  
Policy and Procedure Manual

Signature of Approval

*James B. Runk* 10/11/19  
Tribal Ogema Date

**IT-1100**

**Network and Application Access Policy**

**Purpose**

The purpose of this policy is to define the standard methodology used to create USERID's and assignment of network, application and user access.

**Policy**

**Information Technology Network (ITN):**

It shall be the policy of the Tribal Government of the Little River Band of Ottawa Indians (LRBOI) to limit access to the Tribal Government information technology network (ITN) to the maximum extent possible. When granted, access shall be limited to minimum necessary to accomplish the tasks, duties or responsibilities assigned. All persons authorized access to the ITN shall have a unique USERID and password created within the requirements of this policy and IT-0100 Network Password Policy.

The method to request a unique USERID and password will vary depending on the source of the request:

LRBOI Employees:

Immediate Supervisors will generate all requests for unique USERID for the employees they supervise. This includes all new employees, rehires, transferring employees and change of name. Submit all requests to [Helpdesk@lrboi-nsn.gov](mailto:Helpdesk@lrboi-nsn.gov). Include Employee Name, Title, Department, and Office Location, and the reason for the request i.e. New Hire; Name Change; Transfer etc.

**Requests for USERID may take at up to two-business days to process.**

DO NOT include requests for equipment in the request for a USERID. Submit equipment requests separately in the form of Request for Quote. {NOTE: The IT Department does not maintain spare equipment}

LRBOI Employees requiring access to any of the Indian Health Services Systems must use the I.H.S. ITAC form to request that access, and submit via [Helpdesk@lrboi-nsn.gov](mailto:Helpdesk@lrboi-nsn.gov).

Indian Health Service Employees:

All I.H.S. employees requesting access to the LRBOI health system should submit an I.H.S. ITAC form to [Helpdesk@lrboi-nsn.gov](mailto:Helpdesk@lrboi-nsn.gov).

Vendors:

Any Vendor requiring access to the Tribal Government network must request a unique USERID and VPN access via the Program Director that controls or uses the software they are required to support. If access is not for software support the program director must describe what the access is for and why it is necessary. Review IT Policy IT-9010 Remote Network Access and submit the request via [HelpDesk@lrboi-nsn.gov](mailto:HelpDesk@lrboi-nsn.gov) describing the vendor and the access needed and why. The Information Technology Director will review each



**Little River Band of Ottawa Indians**  
Information Technology  
Policy and Procedure Manual

Signature of Approval

Tribal Ogema      Date

Vendor access request on a case-by-case basis. Access granted is at the sole discretion of the Information Technology Director.

Vendor USERID's are active only when scheduled via a [HelpDesk@lrboi-nsn.gov](mailto:HelpDesk@lrboi-nsn.gov) request. One Business day's notification is required. The IT Director on a case-by-case basis handles emergency requests.

Permission to access


The IT Director may grant the individual vendor permission to access the ITN, but does not guarantee access due to vendor equipment failure and/or incompatibility.

Application Software:

The Director of the Program that operates the application software shall control access to the various application software in use throughout the Tribal Government. The Program Directors will be responsible for implementing and enforcing this policy.

**Authority**

As authorized by IT-0000 and the signature of the Ogema on page one of this policy.

Review/Change	Date	Description	Initial
Initial Issue	01 OCT 2019	First Issue	

01 October 2019



**Little River Band of Ottawa Indians**  
Information Technology  
Policy and Procedure Manual

Signature of Approval	
<i>Harry E. Roman</i> 10/12/19	
Tribal Ogema	Date

**IT-1200**  
**Security Incident Response Policy**

**1. Purpose:**

This policy provides a framework for responding to adverse events such as computer viruses, malicious software, hoaxes, vandalism, automated attacks, and intrusions. The purpose is to ensure appropriate action is taken to minimize the consequences of such adverse events and emergency response procedures and responsibilities are documented, understood, and properly executed when necessary.

**2. Background:**

Little River Band of Ottawa Indians (LRBOI) recognizes the need to augment its computer security efforts because of increased threats to critical cyber-based infrastructure systems. Incidents involving cyber threats, i.e., viruses, malicious user activity, and vulnerabilities associated with highly interconnected technology, require a skilled and rapid response before they can cause significant damage to computing resources, loss or destruction of data, loss of funds, loss of productivity, and damage to the LRBOI's reputation. These situations require that the LRBOI have a coordinated computer security incident response capability as an extension to its contingency planning process.

**3. Scope:**

This policy applies to all LRBOI organizational components including but not limited to Legislative Branch, Judicial Branch, Executive Branch and all business or enterprises owned and operated by LRBOI, excepting those enterprises regulated under The Indian Gaming Regulatory Act (Pub.L. 100-497, 25 U.S.C. § 2701 et seq.). This policy applies to all LRBOI Information Technology activities including the equipment, procedures, and technologies that are employed in managing these activities. This policy is applicable to teleworking, travel, other off-site locations, and all LRBOI office locations. LRBOI officials shall apply this policy to contractor personnel, interns, externs, and other non-Government employees by incorporating such reference in contracts or memorandums of agreement as conditions for using Government-provided IT resources. This policy applies to computer security threats initiated by employees (e.g., misconduct) and external components.

**4. Definitions:**

- a. Computer Security Incident. Any event that may result in, or has resulted in, the unauthorized access to, or disclosure of, sensitive or classified information; unauthorized modification or destruction of systems data; reduced, interrupted, or terminated processing capability; malicious logic or virus activity; or the loss, theft, damage,

or destruction of any IT resource. Examples of incidents may include: the unauthorized use of another user's account, unauthorized use of system privileges, execution of malicious code (e.g., viruses, Trojan horses, or back doors), unauthorized scans or probes, successful or unsuccessful intrusions, and insider attacks. Events such as natural disasters and power-related disruptions are not generally within the scope of Incident Response Teams (IRT) and are addressed in the LRBOI's business continuity and contingency plan.

- b. Event. An event is any observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash, and packet flooding within a network.

## **5. Policy:**

It is the policy of LRBOI to ensure that its systems and data are safe and secure from unauthorized access that might lead to the alteration, damage, or destruction of automated resources and data, unintended release of data, interrupted service, and denial of service

## **6. Procedure:**

The following procedures shall be followed to ensure the protection and control of IT resources:

- a. Incident Response Capability. LRBOI shall have an incident response capability to handle virtually any computer security problem that occurs and have the means for reporting incidents and disseminating incident-related information to management and users. In addition, the incident response capability must not only react to incidents, but also must have the resources to alert and educate users to pertinent risks and heighten awareness about security threats and incident-handling procedures.
- b. Incident Response Teams. LRBOI shall establish an Incident Response Team (IRT) to determine the nature and level of severity of a computer security problem, participate in the investigation, and resolve the incident. The IRT shall:
  - i. Consist of the following employees:
    - 1. Operations Lead
    - 2. Medical Lead
    - 3. Information Technology Director
    - 4. Medical Director
    - 5. Unified Legal Staff Attorney
  - ii. Include an IRT Technical Support Team consisting of:
    - 1. Systems Administrator
    - 2. Systems Security Administrator
    - 3. Network Engineer
  - iii. Have the specific technical skills to respond quickly to incidents in a particular environment and geographical location;
  - iv. Report incidents and their status to the Tribal Ogema, and



- v. Keep the Tribal Ogema apprised of events as they unfold; and of ongoing investigations, and prepare a report of findings upon completion of the incident.
- c. Reporting Notifications. Procedures for handling a variety of incidents and notifications shall be documented, including primary and secondary contacts for required reporting notifications, and shall require answers to questions that would permit the IRT to respond in a business-like manner.
- d. Central Point of Contact. LRBOI central point of contact is the Operations Lead for required reporting of incidents, coordinating the Tribal Government's response to an incident, and acting as a clearinghouse for disseminating information on alerts and vulnerabilities.
- e. Activation of the IRT. Shall be at the discretion of the Operations Lead. The Systems Security Administrator shall monitor all computer incidents and report them to the IT Director. The IT Director shall review the reports and report all computer events involving, systematic attacks or a significant loss of dollars, or damage to LRBOI property or image to the Operations Lead. All events impacting operations shall be reported immediately to Operations Lead.
- f. Violation of Law; Criminal Intent. If during the course of an investigation it appears possible that a violation of the law or criminal intent exists, the LRBOI IRT shall inform the Tribal Ogema and report necessary information to law enforcement. The Director of Public Safety shall assume primary responsibility for investigating the alleged violation. The LRBOI IRT shall only be responsible for addressing the technical aspects of the case.
- g. Employee, Contractor, or Other Misconduct. If the LRBOI IRT finds that employee, contractor, or other misconduct caused the incident, the LRBOI IRT shall submit the appropriate documentation to HR office for determination of what actions need to be taken and be responsible for completing the investigation of the employee's case in conjunction with the LRBOI Personnel Manual. LRBOI IRT shall only be responsible for addressing the technical aspects of the case.
- h. Resolved Incident. After the incident has been resolved, a "lessons learned" session shall be conducted so that the LRBOI IRT can learn from the experience and, if necessary, update its procedures. As a result of the post-incident analysis, the LRBOI IRT may need to issue alerts or warnings to its constituency about certain actions to take to reduce vulnerabilities that were exploited during the incident. LRBOI IRT shall use the post-incident analysis to ascertain the impact on Tribal Operations as a result of handling and resolving the incident.

## **7. RESPONSIBILITIES:**

Information systems security responsibilities and accountability shall be explicit. The responsibilities and accountability of owners, providers, and users of computer systems and other parties concerned with the security of information systems shall be documented.

- a. Information Technology Director. LRBOI IT Director is responsible for the following:
  - i. Monitoring and updating the LRBOI security policies, procedures, standards, and architecture to enable better detection and response capability.
  - ii. Notifying LRBOI organizational components and coordinating responses regarding incidents that span more than one organizational unit.
  - iii. Promptly notifying the Operations Support Lead of computer security incidents that are substantial, systematic attacks and/or involve the loss of dollars or damage to LRBOI property or image.
  - iv. Ensuring appropriate procedures are implemented and instructions are issued for the detection and removal of malicious software.
  - v. Ensuring IT security requirements, procedures, and practices are provided in computer security training materials.
- b. Systems Security Administrator. The LRBOI systems security administrator is the person most often responsible for operational security and is responsible for:
  - i. Notifying the LRBOI IT Director of computer security incidents.
  - ii. Developing and disseminating information on the potential dangers of computer security incidents, guidelines for controlling them, and guidelines for reporting incidents.
  - iii. Collecting and reviewing daily incident reports.
  - iv. Ensuring appropriate procedures are developed and implemented, and instructions are issued for the detection and removal of malicious software.
  - v. Ensuring all LRBOI personnel are aware of this policy.
  - vi. Ensuring this policy is incorporated into computer security briefings and training programs.
  - vii. Serving as an LRBOI point-of-contact for incident reporting and subsequent resolution.
  - viii. Ensuring incident reports for all computer-related incidents are sent to the LRBOI IT Director.
- c. Supervisors and Managers. Supervisors and managers shall ensure their staff have an awareness of their security responsibilities for reporting any computer incidents and conveying initial incident reports.
- d. Employees. Employees shall report any suspected or actual computer incidents immediately to their help desk support, Systems Security Administrator, or other designated personnel.
- e. Incident Response Team. The IRT shall participate in the investigation and resolution of incidents which include (but are not limited to) the following:
  - i. Unauthorized access or attempts.
  - ii. Compromise of proprietary data using electronic means.
  - iii. Computer misuse or abuse.

- iv. Loss of data or computer availability sufficient to cause mission or programmatic impact.
- v. Vulnerability of hardware or software.
- f. The IRT is responsible for the following:
  - i. Identifying computer security incidents, characterizing the nature and severity of the incident, and providing immediate diagnostic and corrective actions when appropriate.
  - ii. Considering priorities in evaluating and responding to each incident (the incident may have many possible effects, ranging from the risk to human life and safety to protecting sensitive, proprietary and scientific data) and minimizing the disruption of computing resources.
  - iii. Receiving incident reports from the intrusion detection system, pro-active scans, system administrators, law enforcement officials, and other sources.
  - iv. Incidence Response Team members shall share knowledge by maintaining a report log. If a suspicion is confirmed or indeterminate, the IRT shall start an event log by noting the date and time of all actions, immediately taking a snapshot of the pertinent files of the incident investigation, and informing the Tribal Ogema.
  - v. Preparing a report of findings and performing a post-incident review.

## 8. Authority

As authorized by IT-0000 and the signature of the Ogema on page one of this policy.

Review / Change	Date	Description	Initial
Original	01 OCT 19	First Issue	