

CHUGACH ELECTRIC ASSOCIATION, INC.
Anchorage, Alaska

REGULAR BOARD OF DIRECTORS' MEETING
AGENDA ITEM SUMMARY

October 22, 2008

ACTION REQUIRED

AGENDA ITEM NO. XI.B.

 Information Only
 X **Motion**
 Resolution
 Executive Session
 Other

TOPIC

Board Policy 133 – Identity Theft Prevention Program

DISCUSSION

Title 16 Part 681 et seq. of the Code of Federal Regulations (Red Flag Rule) requires Chugach to implement an Identity Theft Prevention Program (Program) by November 1, 2008. The Program consists of a written Board policy as well as internal Departmental practices and procedures intended to prevent and mitigate theft of an Association member's Personal Identifying Information.

Personal Identifying Information is defined as any name or number that may be used alone or in conjunction with any other information to identify a specific person including:

- (1) Name, social security number, date of birth, official state- or government- issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number
- (2) Unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- (3) Unique electronic identification number, address or routing code; or
- (4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

Proposed Board Policy 133 has been revised to include compliance monitoring and more frequent reporting as suggested and discussing at the October 8, 2008 Operations Committee Meeting.

MOTION

Move that the Board of Directors adopt Board Policy 133, Identity Theft Prevention Program.

CHUGACH ELECTRIC ASSOCIATION, INC.

BOARD POLICY: 133

DATE: _____

IDENTITY THEFT PREVENTION PROGRAM

I. OBJECTIVE

To implement an Identity Theft Prevention Program (Program) as required by Title 16 Part 681 *et seq.* of the Code of Federal Regulations (Red Flag Rule).

II. CONTENT

The Program must include methods for (1) identifying and detecting, (2) preventing and responding to, and (3) mitigating theft of an Association member's Personally Identifying Information (PII). The Program must include the establishment of policies and procedures for:

- Identifying patterns, practices, and specific forms of activity that are Red Flags, which indicate a possible existence of Identity Theft;
- Responding to any Red Flags that are detected to prevent and mitigate Identity Theft;
- Ensuring regular Program updates to reflect changes in risks from Identity Theft;
- Training staff to effectively implement the Program;
- Exercising appropriate and effective oversight of service provider arrangements and;
- Reporting the effectiveness of the Program in annual internal reports.

III. DEFINITIONS

Identity Theft

Fraud committed or attempted using the identifying information of another person without authority.

Personally Identifying Information

Any name or number that may be used alone or in conjunction with any other information to identify a specific person including

- (1) Name, social security number, date of birth, official state- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- (2) Unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- (3) Unique electronic identification number, address or routing code; or
- (4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

Red Flag

A pattern, practice, or specific activity that indicates a possible existence of Identity Theft.

Member

A person, including a non-natural entity, who is a member of the Association.

IV. SCOPE

This Policy applies to all Association personnel including full-time, part-time, and temporary employees; contractors; consultants; vendors; auditors; and others engaged to perform work for or on behalf of the Association with access to member PII that is maintained, stored, or transmitted by the Association and at all physical locations owned, leased, contracted, or otherwise occupied by the Association or its vendors.

V. PROGRAM

The Program consists of this Policy; Departmental Practices and Procedures in Member Services, Administrative Services, Human Resources, and Information Services; and applicable Chugach Operating Policies, e.g., Operating Policy 027.142 Encryption Policy.

A. Member Services

Member Services is the custodian of all Association member PII and grants and revokes access to the Customer Information System (CIS), which hosts all member PII. Member Services maintains detailed procedures and Department Practices consistent with this Policy.

B. Administrative Services

Administrative Services shall ensure that all contracts with third party businesses that use, store, or otherwise may have access to or utilize Association member PII (in any human or machine readable form) meet work practices consistent with this Policy. Additionally, third party businesses shall be contractually obligated to have reasonable alternative safeguards that provide the same or a greater level of protection for Association member information as provided by the Association. Administrative Services maintains detailed procedures and Department Practices consistent with this Policy.

C. Information Services

Information Services develops and hosts the systems that transmit, receive, and store member PII. Information Services maintains detailed procedures and Department Practices consistent with this Policy.

D. Human Resources

Human Resources shall ensure Information Services Help Desk is promptly notified of involuntary termination or suspension of employees.

Human Resources maintains detailed procedures and Department Practices consistent with this Policy.

E. Training

Member Services shall provide training to Association personnel prior to granting his/her permission to access member PII in the CIS. Additionally, training will be provided annually thereafter until his/her CIS access is revoked. A record of those completing training is maintained in the Training database.

F. Reporting

Each Department having responsibility under this Policy shall prepare a quarterly report for the Senior Vice President of Administration on the progress of implementation of the Program; Program effectiveness; the risk level of identity theft of member PII; and contain any suggested revisions to the Program to further protect member PII; compliance results and identification and discussion of instances of Identity Theft of Association member PII. The Senior Vice President of Administration shall review the reports, follow up on any issues raised, and provide a summary to the CEO. The CEO shall review the summary, discuss it with the Senior Vice President of Administration if necessary, and provide a copy of it to the Board. All reports and summaries shall be marked "Confidential".

G. Program Updates

The Association shall at least annually determine whether it has experienced any Identity Theft of member PII; whether changes in the methods of Identity Theft require updates to this Policy; and whether changes to the Policy, Practices and Procedures are necessary to detect, prevent, and mitigate Identity Theft. The Association will continuously monitor changes in the methods of Identity Theft, and will re-evaluate this Policy if changes are identified.

H. Compliance Monitoring

Department Practices and Procedures shall include regular compliance monitoring functions designed to ensure the Program is being carried out as described in this Policy, the Practices and Procedures, including any revisions.

Department Managers responsible for this Policy shall communicate possible revisions that may be needed to the Senior Vice President of Administration and copy all of responsible or affected Department Managers.

VI. RESPONSIBILITY

The Chief Executive Officer shall be responsible for the overall administration of this Policy. The Senior Vice President of Administration shall be responsible for the oversight, development, and administration of the Program. Senior management of Administrative Services, Information Services, and Member Services shall direct and monitor the implementation of appropriate procedures to implement the Program, to update the Program, and provide training as necessary and appropriate, in accordance with this Policy.

Date Approved: _____

Attested: _____

Alex Gimarc
Secretary of the Board

REVIEW & AMENDMENT HISTORY:

This Board Policy should be reviewed at least once every two years. Amendments may occur any time necessary.

Reviewed by	Review Date	Amended by	Amendment Date

To enter data: From the toolbar select "View" and then select "Header and Footer". Right click in the box above and select "Toggle Field Codes". Enter the data. Once complete right click again in the box above and select "Toggle Field Codes". Close the "Header and Footer".

CHUGACH ELECTRIC ASSOCIATION, INC.

BOARD POLICY: 133

DATE: _____

IDENTITY THEFT PREVENTION PROGRAM

I. OBJECTIVE

To implement an Identify Theft Prevention Program (Program) as required by Title 16 Part 681 *et seq.* of the Code of Federal Regulations (Red Flags Rule).

II. CONTENT

The Program must include methods for (1) identifying and detecting, (2) preventing and responding to, and (3) mitigating theft of an Association member's Personally Identifying Information (PII). The Program must include the establishment of policies and procedures for:

- Identifying patterns, practices, and specific forms of activity that are Red Flags, which indicate a possible existence of Identity Theft;
- Responding to any Red Flags that are detected to prevent and mitigate Identity Theft;
- Ensuring regular Program updates to reflect changes in risks from Identity Theft;
- Training staff to effectively implement the Program;
- Exercising appropriate and effective oversight of service provider arrangements and;
- Reporting the effectiveness of the Program in annual internal reports.

III. DEFINITIONS

Identity Theft

Fraud committed or attempted using the identifying information of another person without authority.

Personally Identifying Information

Any name or number that may be used alone or in conjunction with any other information to identify a specific person including

- (1) Name, social security number, date of birth, official state- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- (2) Unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- (3) Unique electronic identification number, address or routing code; or
- (4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

Red Flag

A pattern, practice, or specific activity that indicates a possible existence of Identity Theft.

Member

A person, including a non-natural entity, who is a member of the Association.

IV. SCOPE

This Policy applies to all Association personnel including full-time, part-time, and temporary employees; contractors; consultants; vendors; auditors; and others engaged to perform work for or on behalf of the Association with access to member PII that is maintained, stored, or transmitted by the Association and at all physical locations owned, leased, contracted, or otherwise occupied by the Association or its vendors.

Deleted: staff of business partners;

V. PROGRAM

The Program consists of this Policy; Departmental Practices and Procedures in Member Services, Administrative Services, Human Resources, and Information Services; and applicable Chugach Operating Policies, e.g. Operating Policy 027.142 Encryption Policy.

A. Member Services

Member Services is the custodian of all Association member PII and grants and revokes access to the Customer Information System (CIS), which hosts all member PII. Member Services maintains detailed procedures and Department Practices consistent with this Policy.

B. Administrative Services

Administrative Services shall ensure that all contracts with third party businesses that use, store, or otherwise may have access to or utilize Association member PII (in any human or machine readable form) meet work practices consistent with this Policy. Additionally, third party businesses shall be contractually obligated to have reasonable alternative safeguards that provide the same or a greater level of protection for Association member information as provided by the Association. Administrative Services maintains detailed procedures and Department Practices consistent with this Policy.

C. Information Services

Information Services develops and hosts the systems that transmit, receive, and store member PII. Information Services maintains detailed procedures and Department Practices consistent with this Policy.

D. Human Resources

Human Resources shall ensure Information Services Help Desk is promptly notified of involuntary termination or suspension of employees. Human Resources maintains detailed procedures and Department Practices consistent with this Policy.

E. Training

Member Services shall provide training to Association personnel prior to granting his/her permission to access member PII in the CIS. Additionally, training will be provided annually thereafter until his/her CIS access is revoked. A record of those completing training is maintained in the Training database.

F. Reporting

Each Department having responsibility under this Policy, shall prepare a quarterly report for the Senior Vice President of Administration on the progress of implementation of the Program; Program effectiveness; the risk level of identity theft of member PII; and contain any suggested revisions to the Program to further protect member PII; compliance results and identification and discussion of instances of Identity Theft of Association member PII. The Senior Vice President of Administration shall review the reports, follow up on any issues raised, and provide a summary to the CEO. The CEO shall review the summary, discuss it with the Senior Vice President of Administration if necessary, and provide a copy of it to the Board. All reports and summaries shall be marked "Confidential."

G. Program Updates

The Association shall at least annually determine whether it has experienced any Identity Theft of member PII; whether changes in the methods of Identity Theft require updates to this Policy; and whether changes to the Policy, Practices and Procedures are necessary to detect, prevent, and mitigate Identity Theft. The Association will continuously monitor changes in the methods of Identity Theft, and will re-evaluate this Policy if changes are identified.

H. Compliance Monitoring

Department practices and procedures shall include regular compliance monitoring functions designed to ensure the Program is being carried out as described in this Policy, the practices and procedures, including any revisions.

Department Managers responsible for this Policy shall communicate possible revisions that may be needed to the Senior Vice President of Administration and copy all of responsible or affected Department Managers.

- Deleted: un
- Deleted: Management personnel assigned re
- Deleted: sponsibility under this Policy
- Deleted:
- Deleted: n annual
- Deleted:
- Deleted: ii
- Deleted: k
- Deleted: regarding the implementation
- Deleted: and
- Deleted: , status,
- Deleted:
- Deleted: of the Red Flags program.
- Deleted: The report shall include the following: implementation progress and program effectiveness; ongoing risk level of Identity Theft of member PII; potential program changes to further protect member PII; compliance results; and identification and discussion of instances of Identity Theft of the Association's members. The report will be addressed to the Senior Vice President of Administration
- Deleted: ¶
- Formatted: Indent: Left: 36 pt, Hanging: 36 pt, Numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 27 pt + Tab after: 45 pt + Indent at: 45 pt, Tabs: 72 pt, List tab + Not at 45 pt
- Formatted: Bullets and Numbering
- Deleted: Management personnel assigned responsibility under this Policy shall ensure
- Deleted: in department practices and procedures
- Deleted: ¶
- Formatted: Font: Bold
- Deleted: pr
- Deleted: documented
- Deleted: and in accordance with this policy.
- Deleted: ¶
- Deleted: ve Services
- Deleted: In addition, potential changes to this Policy shall be discussed at least annually. Material changes to this ... [1]

VI. RESPONSIBILITY

The Chief Executive Officer shall be responsible for the overall administration of this Policy. The Senior Vice President of Administration shall be responsible for the oversight, development, and administration of the Program. Senior management of Administrative Services, Information Services, Human Resources, and Member Services shall direct and monitor the implementation of appropriate procedures to implement the Program, to update the Program, and provide training as necessary and appropriate, in accordance with this Policy.

Date Approved: _____

Attested: _____

Alex Gimarc
Secretary of the Board

REVIEW & AMENDMENT HISTORY:

This Board Policy should be reviewed at least once every two years. Amendments may occur any time necessary.

<u>Reviewed by</u>	<u>Review Date</u>	<u>Amended by</u>	<u>Amendment Date</u>

To enter data: From the toolbar select "View" and then select "Header and Footer". Right click in the box above and select "Toggle Field Codes". Enter the data. Once complete right click again in the box above and select "Toggle Field Codes". Close the "Header and Footer".

In addition, potential changes to this Policy shall be discussed at least annually. Material changes to this Policy that may be needed shall be brought to the attention of the Senior Vice President of Administration