

AGENDA

RULES MEETING OF THE BOARD OF TRUSTEES VILLAGE OF PARK FOREST, COOK AND WILL COUNTIES, ILLINOIS

Village Hall

8:00 p.m.

July 13, 2009

Roll Call

1. Intergovernmental Agreement-Interoperable Radio Communication
2. Resolution Authorizing the Approval of Identify Theft Prevention Policy

Mayor's Comments

Manager's Comments

Trustee's Comments

Attorney's Comments

Audience to Visitors

Adjournment

Agenda Items are Available in the Lobby of Village Hall

AGENDA BRIEFING

DATE: July 1, 2009

TO: Mayor John Osteburg
Board of Trustees

FROM: Robert H. Wilcox, Fire Chief

RE: Intergovernmental Agreement - Interoperable Radio Communications

BACKGROUND/DISCUSSION: In 2006, the U.S. Department of Homeland Security's Urban Area Security Initiative (UASI) Working Group, The Office of the President of the Cook County Board of Commissioners, Cook County Sheriff's Department and the City of Chicago presented a plan to provide interoperable communications systems for First Responders throughout Cook County. The goal of this project is to establish an affordable, easy-to-use radio system that will ensure every municipality in Cook County can establish and maintain voice communication with neighboring jurisdictions during an emergency situation.

This collaborative initiative is near completion. The component now available for use and deployment by Village of Park Forest First Responders is Four Portable Radio units, two for police and two for fire, with mobile mounted chargers (including installation) installed in any first responder vehicles we select. The radios would be deployed in command vehicles and would provide for Interoperability between Cook County and Numerous State Agencies through Starcom in the event of an emergency requiring interoperable communications. These radios will also have select Cook County Sheriff's Radio Channels, and the Starcom 21 Channels, which allow for Statewide Interoperability.

The initial cost to install the new County owned equipment in all four vehicles will be covered by this initiative without charge to the Village. The equipment will remain titled to Cook County.

The annual shared radio network maintenance fee for each radio is \$240.00; or an annual total of \$1,200 for four portables and one base station. Should Cook County be able to acquire funding during the initial years of the project, this fee will be reduced accordingly.

The portable and base station equipment provided is covered under warranty for the first three (3) years, when a warranty plan is purchased after the three year term; the exact pass thru cost will be quoted and passed thru to the Village. The estimated cost for each individual radio after the warranty has expired is \$85.00 per year.

RECOMMENDATION: The fire and police departments are recommending the Board authorize the execution of the attached Intergovernmental Agreement for "Public Safety Interoperable Communications Radio Loan Program" between the Village of Park Forest and Cook County.

SCHEDULE FOR CONSIDERATION: This item will appear on the agenda of the Rules Meeting of July 13, 2009, for Board discussion.

COOK COUNTY URBAN AREA WORKING GROUP INTEROPERABLE RADIO COMMUNICATIONS SUBCOMMITTEE

COUNTYWIDE RADIO COMMUNICATIONS INTEROPERABILITY COMMUNICATIONS PLAN - PHASE ONE

Fax Request to Cook County Sheriffs Department Radio Unit: 708-865-4718

Radio Request Form

Date of Request: July 13, 2009

Requesting : One portable radio

Agency: Village of Park Forest

Telephone: 708-748-5605

Contact: Robert H. Wilcox, Fire Chief

Fax: 708-748-4890

Address: 156 Indianwood Blvd.

Email: rwilcox@vopf.com

Town: Park Forest

Zip: 60466

Department Request

Police Department ()
Fire Department (X)
Communications Center ()

Memorandum of Understanding Executed and Attached ()

Vehicle Description for Radio and Mobile Charger Installation

Year: 2006 Make: Ford Model: Expedition Unit#: 70

VIN: 1FMPU16586L Vehicle Contact Person: Robert H. Wilcox

Contact Telephone: 708-748-5605

Person Requesting: Robert H. Wilcox Title: Fire Chief Date: July 13, 2009

COOK COUNTY URBAN AREA WORKING GROUP INTEROPERABLE RADIO COMMUNICATIONS SUBCOMMITTEE

COUNTYWIDE RADIO COMMUNICATIONS INTEROPERABILITY COMMUNICATIONS PLAN - PHASE ONE

Fax Request to Cook County Sheriffs Department Radio Unit: 708-865-4718

Radio Request Form

Date of Request: July 13, 2009

Requesting : One portable radio

Agency: Village of Park Forest

Telephone: 708-748-5605

Contact: Robert H. Wilcox, Fire Chief

Fax: 708-748-4890

Address: 156 Indianwood Blvd.

Email: rwilcox@vopf.com

Town: Park Forest

Zip: 60466

Department Request

Police Department ()
Fire Department (X)
Communications Center ()

Memorandum of Understanding Executed and Attached ()

Vehicle Description for Radio and Mobile Charger Installation

Year: 2008 Make: Ford Model: F-250 Pick Up Unit#: 71

VIN: 1FTSW21R08EE12319 Vehicle Contact Person: D/C Bruce Ziegler

Contact Telephone: 708-748-5605

Person Requesting: Robert H. Wilcox Title: Fire Chief Date: July 13, 2009

COOK COUNTY URBAN AREA WORKING GROUP INTEROPERABLE RADIO COMMUNICATIONS SUBCOMMITTEE

COUNTYWIDE RADIO COMMUNICATIONS INTEROPERABILITY COMMUNICATIONS PLAN - PHASE ONE

Fax Request to Cook County Sheriffs Department Radio Unit: 708-865-4718

Radio Request Form

Date of Request: July 13, 2009

Requesting : One portable radio

Agency: Village of Park Forest

Telephone: 708-748-4700

Contact: Cliff Butz, Deputy Police Chief

Fax: 708-

Address: 200 Lakewood Blvd.

Email: cbutz@vopf.com

Town: Park Forest

Zip: 60466

Department Request

Police Department (X)

Fire Department ()

Communications Center ()

Memorandum of Understanding Executed and Attached ()

Vehicle Description for Radio and Mobile Charger Installation

Year: Vehicle To Be Determined Make: Model: Unit#:

VIN: Vehicle Contact Person:

Contact Telephone:

Person Requesting:

Title:

Date:

**COOK COUNTY URBAN AREA WORKING GROUP
INTEROPERABLE RADIO COMMUNICATIONS SUBCOMMITTEE**

**COUNTYWIDE RADIO COMMUNICATIONS INTEROPERABILITY COMMUNICATIONS
PLAN - PHASE ONE**

Fax Request to Cook County Sheriffs Department Radio Unit: 708-865-4718

Radio Request Form

Date of Request: July 6, 2009

Requesting : One portable radio

Agency: Village of Park Forest

Telephone: 708-748-4700

Contact: Cliff Butz, Deputy Police Chief

Fax: 708-

Address: 200 Lakewood Blvd.

Email: cbutz@vopf.com

Town: Park Forest

Zip: 60466

Department Request

Police Department (X)

Fire Department ()

Communications Center ()

Memorandum of Understanding Executed and Attached ()

Vehicle Description for Radio and Mobile Charger Installation

Year: Vehicle To Be Determined Make: Model: Unit#:

VIN: Vehicle Contact Person:

Contact Telephone:

Person Requesting:

Title:

Date:

INTERGOVERNMENTAL AGREEMENT

PUBLIC SAFETY INTEROPERABLE COMMUNICATIONS RADIO LOAN

This INTERGOVERNMENTAL AGREEMENT (the "Agreement") is entered into as of _____, 2009 (the "Effective Date") by and between the County of Cook (the "County"), a public body corporate of the State and home rule unit of government under Article VII, Section 6(a) of the 1970 Constitution of the State of Illinois, on behalf of the Cook County Sheriff, ("Sheriff"), and The Village of Park Forest (the "Recipient"), a unit of local government of the State of Illinois.

RECITALS:

WHEREAS, the County and Recipient are part of a regional collaboration to enhance interoperable public safety communications capabilities throughout Cook County; and

WHEREAS, the Illinois Emergency Management Agency ("IEMA") has received various grant funds from the U.S. Department of Homeland Security, to support interoperable communications projects within the State; and

WHEREAS, in 2007, the IEMA awarded grant funding to the County to accomplish certain projects, including: (1) Upgrading the County's digital trunked radio system ("Digital Trunked System") to be P25 standard compliant (including the connection of County and municipal radios to the State of Illinois' StarCom 21 system, thereby allowing state-wide communication) and (2) Providing links from the County's Digital Trunked System to achieve interoperability with radio systems belonging to participating entities such as Recipient; and

WHEREAS, the County and Recipient believe that the goal of enhancing interoperable public safety communications capabilities within Cook County would be served by the loan by the County to Recipient of certain portable radios belonging to the County for the use of Recipient's public safety agencies, including, but not limited to, its police and fire departments on the terms more fully described herein; and

WHEREAS, Article VII, Section 10 of the Constitution of the State of Illinois authorizes and encourages units of local government to contract or otherwise associate among themselves to obtain or share services and to exercise, combine or transfer any power or function.

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the parties hereto hereby agree as follows:

SECTION 1: INCORPORATION OF RECITALS

The recitals set forth above are incorporated in this Agreement by reference and made a part of this Agreement.

SECTION 2: GRANT OF RIGHTS

Pursuant to this agreement, the County, acting through the Sheriff, shall make available to Recipient up to four (4) portable radios ("Radios"), which are and shall at all times be considered the property of the County. The specific quantity, type, model and any other pertinent characteristics of the Radios made

available to Recipient shall be set forth on an addendum to this agreement, which shall be in the form and substance as Attachment 1, attached to this Agreement and be incorporated into this Agreement without need for further action by either party. At any time during the course of this Agreement, the County may request the return of less than all of the Radios made available to Recipient pursuant to this Agreement and Recipient shall promptly comply with the County's request.

Accordingly, the County hereby grants to Recipient, upon the terms and conditions herein specified, permission to use the Radios for Recipient's official purposes, including, but not limited to, the purpose of enhancing Recipient's ability to achieve interoperable communications with the County and other public safety entities.

Recipient shall have no right to transfer, assign, sublease, or confer any rights or benefits with respect to the use of the Radios to any third party without the written permission of the County.

SECTION 3: TERM AND TERMINATION; EFFECTS OF TERMINATION

3.1 Term and Termination

This Agreement shall commence upon the date upon which both parties have duly executed it (the "Effective Date") and shall continue thereafter until terminated by either party. Either party wishing to terminate this Agreement may do so for any reason upon ninety (90) days written notice to the other.

A request by the County, pursuant to Section 2, Grant of Rights for a return of less than all of the Radios made available to Recipient pursuant to this Agreement shall not automatically operate to terminate this Agreement.

3.2 Effects of Termination

Effective upon the date of termination specified in writing by party terminating this Agreement: (1) Recipient's right to use the Radios shall cease; (2) Recipient's obligation to pay the Fees described in Section 5.2, Recipient, herein, shall cease; and (3) Recipient shall promptly return the Radios to the County.

SECTION 4: CONTROL OF RESPECTIVE RADIO SYSTEMS

The County and its Sheriff have ultimate authority with regard to the County's Digital Trunked System. Recipient shall have ultimate authority over its own radio system. It is agreed by the parties that the County's Digital Trunked System is and shall remain under full control and supervision of the Sheriff and that the County is and shall be the sole owner of its existing Digital Trunked System as well as any new, added equipment that may in the future be made a part of the County's Digital Trunked System and other County networks or property. This status shall include all towers, radio equipment, connections, generators, computers, and all other such attachments and appurtenances.

It is further understood and agreed that Recipient is and shall be the sole owner of all of its existing radio system as well as any new, added equipment that may in the future be made a part of the Recipient's radio system and other Recipient networks or property, provided, however, that County-owned equipment that may be installed at Recipient locations to make connections to the Digital Trunked System is and shall remain the County's property and shall not be disturbed.

SECTION 5: RESPONSIBILITIES OF THE PARTIES

5.1 The County

5.1.1 Delivery and Installation of Radios

Pursuant to a mutually agreed upon schedule, the County shall deliver the Radios described in Attachment 1 to Recipient and shall install the Radios in public safety first responder vehicles designated by Recipient. County shall not be responsible for any additional Radio installations and shall not be obligated to install a Radio if it determines, in its sole discretion, that the vehicle provided by Recipient is unsuitable for such installation.

5.1.2 Training

Pursuant to a mutually agreed upon schedule, the County shall provide training on the use and operation of the Radios to the appropriate Recipient personnel who will be responsible for such operation.

5.1.3 Radio Frequencies; Access Codes

The County shall provide Recipient with the appropriate licensed frequencies upon which the Radios shall be used and shall provide updated or alternative frequencies as such frequencies become applicable. County shall also provide Recipient with any applicable access codes pursuant to which the Radios may be used to access the Digital Trunked System.

5.1.4 Direct Costs

The County shall be responsible for those costs associated with the core operations of its Digital Trunked System (the "Direct Costs"), which include the following:

- A. Maintenance costs for Digital Trunked System expenses that are directly billed to the County by the providers of such maintenance services;
- B. Telephone and utility costs and expenses;
- C. Direct labor costs of County Digital Trunked System technicians, engineers and other personnel assigned to the ongoing use of the Digital Trunked System;
- D. Other costs which are directly attributable to the cost of the Digital Trunked System, excluding rental costs.

5.2 Recipient

5.2.1 Monthly Access Fee

Recipient shall pay the County a monthly fee in exchange for the right to access the Digital Trunked System. This fee shall be calculated as follows:

The total dollar-for-dollar amount of the Direct Cost items listed in Section 5.1.3, Direct Costs, above, divided by the total number of Users* on the Digital Trunked System multiplied by the total number of

Recipient Users (Monthly Access Fee = Direct Costs ÷ total number of Users on Digital Trunked System × total number of Recipient Users). The actual costs and quantities employed in the formula used to calculate the Monthly Access Fee are set forth in Attachment 2, attached to this Agreement. Attachment 2 will be updated by the County from time to time as the applicable costs and quantities change, but no less than annually.

* For purposes of this Section 5.2, a “User” means an individual, active or assigned radio user identification number for a radio programmed to be operational on the Digital Trunked System, whether or not it is a Radio subject to this Agreement. Radio user identification numbers assigned to inactive or reserve radios that are not programmed to be operational on the Digital Trunked System are not included in this definition.

5.2.2 Reimbursements

Recipient shall reimburse the County for costs incurred by the County as a result of purchases made by the County at the request of and for the benefit of Recipient. These costs may either be billed to the Recipient by the County or billed directly to the Recipient by the applicable vendor and include, but are not limited to, the following:

- A. Per unit maintenance costs associated with Recipient’s Users that are billed directly as a per-unit cost;
- B. Programming, re-programming, or other expenses associated with the maintenance of Recipient’s Users;
- C. Installation or re-installation costs of equipment that requires permanent installation;
- D. Special equipment, service, or connections for which only Recipient directly benefits.

5.3 Use of Radios

Recipient shall use the Radios only for official purposes and shall keep each Radio tuned at all times to the licensed interoperable frequencies designated by the Sheriff. Recipient shall conduct a monthly test of each Radio that will evidence to the Sheriff that the Radio is operational and tuned to the correct frequency. Recipient shall ensure that any access codes provided by the County shall only be given to those authorized by the County to receive them.

5.4 Cooperation and Access

Throughout the term of this Agreement, Recipient shall provide the County with reasonable cooperation and access to its facilities to promote the delivery and installation of the Radios, the training of the Recipient’s personnel and any other purposes of this Agreement.

5.5 Risk of Loss; Insurance

Upon the installation of the Radios in Recipient’s vehicles or upon its premises, Recipient shall bear the risk of loss for any damage or loss to such Radios. Accordingly, throughout the term of this Agreement, Recipient shall procure and maintain property insurance that shall provide coverage against all risks of physical loss and/or damage on a full replacement cost valuation basis without deduction for

depreciation. Such insurance shall list Cook County as a named insured and loss payee.

5.6 Release and Indemnification; Covenant not to Sue

A. Release and Indemnification

Recipient is not purchasing the Radios and is making any payment to the County to reimburse the County for the County's purchase of the Radios. In entering into this Agreement, County seeks to enhance the ability of Recipient and its first responders to communicate and respond to threats or emergencies. Accordingly, in consideration of the terms and conditions of this Agreement, with the exception of intentional torts committed by County, Recipient hereby releases and agrees to indemnify and hold harmless the County, and all of its present, former and future officers, commissioners, employees, attorneys, agents and assigns from and against any and all losses, liabilities, damages, claims, demands, fines, penalties, causes of action, costs and expenses whatsoever, including, but not limited to, attorneys' fees and court costs, present or future, known or unknown, sounding in law or equity that arise out of or from or otherwise relate, directly or indirectly, to this Agreement or to the use of the Digital Trunked System.

B. Covenant Not to Sue

Recipient hereby covenants and agrees that it shall not sue, institute, cause to be instituted or permit to be instituted on its behalf, or by or on behalf of its past, present or future officials, officers, shareholders, directors, partners, employees, attorneys, agents or assigns, any proceeding or other action with or before any local, state and/or federal agency, court or other tribunal, against the County, its officers, commissioners, employees, attorneys, agents or assigns, arising out of, or from, or otherwise relating, directly or indirectly, to this Agreement.

SECTION 6: MISCELLANEOUS TERMS

6.1 No Joint Venture

This Agreement shall in no event be construed in such a way that either County or Recipient constitutes, or is deemed to be, the representative, agent, employee, partner, or joint venturer of the other. The parties shall not have the authority to enter into any agreement, nor to assume any liability, on behalf of the other party, nor to bind or commit the other party in any manner, except as expressly provided herein.

6.2 Notice

All notices required to be given pursuant to this Agreement shall be in writing and addressed to the parties at their respective addresses set forth below. All such notices shall be deemed duly given if personally delivered, or if deposited in the United States mail, registered or certified return receipt requested, or upon receipt of facsimile transmission. Notice given as provided herein does not waive service of summons or process.

If to the County, to:

Office of the Cook County Sheriff

1401 N. Maybrook Dr.

Maywood, IL 60153

Attention: Chief of Police

Telephone: (708) 865-6520

Facsimile: (708) 865-4718

If to Recipient, to:

Park Forest Fire Department

156 Indianwood Blvd.

Park Forest, IL 60466

Attention: Robert H. Wilcox, Fire Chief

Telephone: 708-748-5606

Facsimile: 708-748-4890

6.3 Entire Agreement

This Agreement constitutes the entire agreement of the County and Recipient with respect to the subject matter hereof and supersedes all other prior and contemporary agreements, understandings, representations, negotiations, and commitments between Recipient and County with respect to the subject matter hereof.

6.4 Approval Required and Binding Effect

This Agreement between County and Recipient shall not become effective unless authorized by the County. This Agreement constitutes a legal, valid and binding agreement, enforceable against Recipient and, once duly authorized and executed as set forth herein, against the County.

6.5 Representations

Recipient represents that it has the authority to enter into this Agreement and undertake the duties and obligations contemplated by this Agreement and that it has taken or caused to be taken all necessary action to authorize the execution and delivery of this Agreement.

WHEREFORE, the parties have signed and executed this Agreement as of the date written below in the County of Cook, State of Illinois.

FOR COUNTY:

FOR RECIPIENT:

_____ Date: _____

_____ Date: _____

Tom Dart
Cook County Sheriff

Thomas K. Mick
Village Manager, Village of Park Forest

APPROVED AS TO FORM:

Assistant State's Attorney

MEMORANDUMx

TO: Mayor John Ostenburg
Board of Trustees

FROM: Thomas K. Mick, Village Manager

SUJECT: Identity Theft Prevention Policy

DATE: July 8, 2009

BACKGROUND/DISCUSSION:

To comply with rules established by the Federal Trade Commission related to identity theft protection, municipal agencies are mandated to adopt policies designed to protect consumer's personal information.

Attached is an enabling resolution which establishes Red Flag Rules related to mitigating the potential for identity theft in the operations carried out by the Village of Park Forest.

SCHEDULE FOR CONSIDERATION:

This issue will be on the agenda for the July 13, 2009 Rules Meeting for Board discussion.

MEMORANDUM

DATE: June 24, 2009

TO: Mary Dankowski, Finance Director

FROM: Stephanie Rodas, Assistant Finance Director

RE: Identity Theft Prevention Policy

In 2008, the Federal Trade Commission (FTC) adopted its Red Flags identity theft rules (16 CFR Part 681). The rules were adopted in response to the 2003 amendment of the Fair Credit Reporting Act which required, among other things, that financial institutions and creditors adopt what are called “Red Flag” rules to help protect consumers against identity theft. The term Red Flag means a pattern, practice or specific activity that indicates the possible existence of identity theft. Congress wants all financial institutions and creditors to adopt programs to identify, prevent and mitigate the danger of identity theft to consumers.

Although municipalities are not the focus of this federal legislation, the requirement applies to all “creditors” which under the Act includes “Any person who regularly extends, renews or continues credit”. The term “person” is defined to include governmental subdivisions and agencies. The term “credit” is defined to include the right granted by a creditor to a debtor to “purchase property or services and defer payment.” Because municipal utilities provide water to their customers in advance of being billed for that water, municipal utilities are considered to be creditors falling within the requirements of the Act.

The attached policy was assembled after review of several samples shared by various organizations. Water Department staff attended training in March of 2009 on the Red Flag Rules. The FTC requires the development and implementation of written identity theft prevention programs by August 1, 2009.

On a separate note, this Rule has also been interpreted to apply to the ambulance industry. Andres Medical Billing, our ambulance billing provider adopted an Identity Theft Prevention Program earlier this year.

RESOLUTION No. _____

**RESOLUTION AUTHORIZING THE APPROVAL OF
IDENTITY THEFT PREVENTION POLICY**

WHEREAS, The Village of Park Forest desires to adopt a written Identity Theft Prevention Program (“Program”) to establish rules and procedures to detect, prevent and mitigate identity theft; and

WHEREAS, the Program also meets the requirements of, and brings the Village into compliance with, certain identity theft prevention laws and regulations, including those promulgated by the Federal Trade Commission;

NOW, THEREFORE, BE IT RESOLVED by the Mayor and Board of Trustees of the Village of Park Forest, as follows:

SECTION 1: Recitals. The foregoing recitals are incorporated herein as if fully set forth.

SECTION 2: Adoption of Policy. The “Identity Theft Prevention Policy,” attached to this Resolution as **Exhibit A**, establishing rules and procedures to detect, prevent and mitigate identity theft (“*Program*”) shall be, and it is hereby, approved.

SECTION 3: Effective Date. This Resolution and the Program shall be in full force and effect upon its passage and approval.

PASSED this _____ day of _____, 2009.

APPROVED:

ATTEST:

Mayor

Village Clerk

Exhibit A

The Village of Park Forest
Identity Theft Prevention Policy

Effective July 2009

I. BACKGROUND

Identity theft has become the number one consumer fraud issue in the country. In 2007, more than 10,000 identity theft complaints were filed with the Federal Trade Commission (“FTC”) by Illinois residents. The Village of Park Forest (“Village”) recognizes that the risk to the Village, its employees, residents, and customers from data loss and identity theft is a significant concern to the Village, which this Identity Theft Prevention Program (“Program”) seeks to address.

II. PROGRAM ADOPTION

The Village developed the Program in an effort to battle identity theft. The Program was developed with oversight and approval of the Mayor and Board of Trustees of the Village. After consideration of the size and complexity of the Village’s operations and customer account systems, and the nature and scope of the Village’s activities, the Mayor and Board of Trustees determined that this Program was appropriate for the Village, and therefore approved the Program in July, 2009.

III. PROGRAM PURPOSE

The Village adopts the Program to help protect employees, customers, contractors, and itself from harm and damage related to, or caused by, the loss or misuse of sensitive information. The Program also will assist the Village in detecting, preventing, and mitigating identity theft. The Program does so by identifying certain “red flags” that suggest or indicate the possibility of identity theft, and by providing guidelines on how the Village should respond once it detects any such Red Flags. Further, the Program will:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper;
3. Describe the electronic security of data when stored and distributed; and
4. Place the Village in compliance with state and federal law regarding identity theft protection.

The Program has been tailored to the size, complexity and the nature of the Village’s operations. The Program also has been designed in order to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Allow the Village to respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

4. Ensure that the Program is reviewed periodically, and updated, if necessary, to reflect changes in risks to customers or to the safety and soundness of the Village from identity theft.

IV. PROGRAM DEFINITIONS

1. "Covered Account" means: (i) an account that the Village offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a utility account; and (ii) any other account that the Village offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Village, including financial, operational, compliance, reputation, or litigation risks.
2. "Credit" means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
3. "Creditor" means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit, including utility companies.
4. "Customer" means a person that has a covered account with a creditor.
5. "Identity Theft" means a fraud committed or attempted using identifying information of another person without authority.
6. "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
7. "Sensitive Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to, a person's credit card account information, debit card information, bank account information, drivers' license information, social security number, mother's birth name, date of birth, electronic identification number, computer Internet Protocol address, and routing code.
8. "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
9. "Service Provider" means a person that provides a service directly to the Village.

V. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the Village considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The Village identifies the following Red Flags, in the following listed categories:

A. Notifications and Warnings From Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or otherwise inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other documentation with information that is not consistent with existing customer information (e.g. a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (e.g. inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (e.g. an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (e.g. an invalid phone number or an answering service, or fictitious billing address, mail drop or prison);
5. Social security number presented that is the same as one given by another customer;

6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (e.g. very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the Village that a customer is not receiving mail sent by the Village;
6. Notice to the Village that an account has unauthorized activity;
7. Breach in the Village's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the Village from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

VI. DETECTING RED FLAGS.

A. New Covered Accounts

In order to try and detect any of the Red Flags identified in Section V above associated with the opening of a new Covered Account, Village personnel should take the following steps to obtain and verify the identity of the person opening the Covered Account:

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (e.g. review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer if appropriate.

B. Existing Covered Accounts

In order to detect any of the Red Flags identified in Section V above for an existing Covered Account, Village personnel will take the following steps to monitor transactions with a Covered Account:

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email, or otherwise);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

VII. PREVENTING AND MITIGATING IDENTITY THEFT

A. Securing Sensitive Information

Village personnel are encouraged to use common sense judgment in securing sensitive and confidential information. Furthermore, in exercising such judgment, consideration should be given to the Illinois Freedom of Information Act ("FOIA"). If an employee is uncertain of the sensitivity of a particular piece of information, the employee should contact their supervisor or the Program Administrator. Further, if the Village receives a FOIA or other request seeking Sensitive Information, or documents containing Sensitive Information, said requests should be forwarded to the Village Manager and the Village Attorney.

In order to further prevent the likelihood of Identity Theft occurring with respect to Village accounts, the Village shall make reasonable efforts to take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Take steps to ensure that the Village's website is secure or provide clear notice that the website is not secure;
2. Attempt to ensure destruction of paper documents and computer files containing Sensitive Information;
3. Keep file cabinets, desk drawers, cabinets, and any other storage space containing documents with Sensitive Information locked when not in use;

4. Lock storage rooms containing documents with Sensitive Information and record retention area at the end of the work day or when unsupervised.
5. Attempt to ensure that office computers with access to Covered Accounts and/or Sensitive Information are password protected and that computer screens lock after a set period of time;
6. Keep workstations, work areas, and offices clear of papers containing Sensitive Information;
7. Request only the last 4 digits of social security numbers (if any);
8. Attempt to ensure that computer virus protection is up to date;
9. Require and keep only the kinds of Sensitive Information that are necessary for the Village's purposes; and
10. Account statements and receipts for Covered Accounts shall only include the last four digits of the credit card, debit card, or the bank account used for payment of the covered account.

B. Electronic Distribution

Each employee, service provider, or contractor performing work for the Village will comply with the following policies:

1. With respect to internal electronic distribution, Sensitive Information may be transmitted using approved Village electronic mail.
2. With respect to external electronic distribution, Sensitive Information should only be transmitted in an encrypted format and should contain a statement such as this:

"This message may contain sensitive, confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited".

C. Responses When Red Flags Detected

In the event Village personnel detect any identified Red Flags, such personnel should take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to Covered Accounts;

4. Decline or otherwise refuse to open a new Covered Account;
5. Close an existing Covered Account;
6. Reopen a Covered Account with a new number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

VIII. PROGRAM UPDATES

This Program will be periodically reviewed and updated to try and reflect changes in risks to customers and the soundness of the Village from Identity Theft. At least once a year, the Program Administrator will consider the Village's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Village maintains and changes in the Village's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the Mayor and Board of Trustees with his or her recommended changes and the Mayor and Board of Trustees will make a determination of whether to accept, modify or reject those changes to the Program.

IX. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Assistant Finance Director acting as the Program Administrator. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Village staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Village staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Further training shall also be provided on a yearly basis or as needed to address changes in the Program.

C. Service Provider Arrangements

In the event the Village engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the Village will take the following steps to ensure the Service Provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that Service Providers have such policies and procedures in place; and
2. Require, by contract, that Service Providers review the Village's Program and report any Red Flags to the Program Administrator.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Village's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Program Administrator and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general Red Flag detection, implementation and prevention practices are listed in this document.

**Village of Park Forest
Identity Theft Program and Prevention Policy
Red Flag Rules**

I, _____ have received a copy of the Village of Park Forest Identity Theft Program and Prevention Policy. I have read the document and understand the requirements necessary to abide by the policy.

Signature

Print Name

Date