GLENCOE

SMALL CITY BIG FUTURE

GLENCOE CITY COUNCIL MEETING AGENDA

October 7, 2024

City Center Ballroom

7:00 PM

1. **PLEDGE OF ALLEGIANCE AND MOMENT OF SILENCE**

2. **CONSENT AGENDA**
   - **A.** Approve Minutes of the Regular Meeting of September 16, 2024 – Note Change in Resolution 2024-11 – reduction due to addition error.
   - **B.** Special Event Application of **JL Insurance Advisors**, 1132 Hennepin Avenue, Street Closure S 1/2 of 12 Street East of Hennepin Avenue for Customer Appreciation and Chamber of Commerce Ribbon Cutting. October 15, 2024 from 8:00 AM to 11:00 AM. Cones, Barricades and Picnic Tables.
   - **C.** Special Event Application of **Glencoe Days Committee** for Oak Leaf Park – Shelters 1 and 2 for Haunted Harvest Event at Oak Leaf Park, 200 DeSoto Avenue South October 18-19, and October 25-26. Requesting the use of Shelters 1 and 2 for duration of event requiring shelters to be closed for rental, parking, and staff cleanup.

3. **APPROVE AGENDA**

4. **PUBLIC COMMENT (agenda items only)**

5. **PUBLIC HEARINGS**
   - **A.** None Scheduled

6. **BIDS AND QUOTES**
   - **A.** None Scheduled

7. **REQUESTS TO BE HEARD**
   - **A.** FFA Signage Request – Glencoe FFA
   - **B.** Police Policy Change- FBI Criminal Justice Information Services (CJIS) security – Chief Padilla
   - **C.** **Resolution 2024-12** Designating Election Judges and polling place for General Election on November 5th, 2024 – City Administrator
   - **D.** **2025** Prosecuting Attorney Fee Increase request – City Administrator

8. **ITEMS FOR DISCUSSION**
   - **A.** Reminder of City Council Date Change for General Election to November 6, 2024 at 7:00 PM
   - **B.** Revolve Labs update – City Attorney Ostlund

9. **ROUTINE BUSINESS**
   - **A.** Project Updates
   - **B.** Economic Development
   - **C.** Public Input
   - **D.** Reports
   - **E.** City Bills

10. **ADJOURN**

GLENCOE
SMALL CITY & BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

GLENCOE

SMALL CITY BIG FUTURE

GLENCOE CITY COUNCIL MEETING MINUTES
September 16, 2024 – 7:00 PM
City Center Ballroom

Attendees: Ryan Voss, Susan Olson, Mark Hueser, Paul Lemke, Cory Neid, Yodee Rivera

City Staff: Mark Larson, Mark Ostlund, Mark Lemen, Tony Padilla, Todd Trippel, Haylie Kusler, Myranda VanDamme

Absent: Jamie Voigt

Others: Owen Elle, Lowell Anderson, Richard Glennie, Al Robeck

1. **PLEDGE OF ALLEGIANCE AND MOMENT OF SILENCE**
   The Meeting was called to order by Mayor Voss.

2. **CONSENT AGENDA**
   - **A.** Approve Minutes of the Regular Meeting of September 3, 2024
   - **B.** Approve Family Fun Festival Special Event application, closure of the south 1/2 of Taylor Avenue, between 10th and 11th Street, and use of Picnic Tables on Thursday, October 24, 2024.
   - **C.** Approve Homecoming Parade, Friday, September 20, 2024 (Application to follow)

   Motion: Hueser, seconded by Neid. All in favor, the motion carries.

3. **APPROVE AGENDA**
   Remove 9. F. Close meeting for discussion of real estate transaction.
   Motion: Lemke, seconded by Olson. All in favor, the motion carries.

4. **PUBLIC COMMENT (agenda items only)**
   None.

5. **PUBLIC HEARINGS**
   None.

6. **BIDS AND QUOTES**
   - **A.** Set Public Hearing for Delinquent Bills owed to the City of Glencoe for October 21, 2024, at 7:00 PM – City Administrator

   Motion: Lemke, seconded by Hueser to set the public hearing for delinquent bills owed to the City of Glencoe for October 21, 2024, at 7:00 PM. All in favor, the motion carries.

7. **REQUESTS TO BE HEARD**

A. Park Board Recommendation on long-term campground rentals – City Administrator

Motion: Lemke, seconded by Olson to approve the Park Board recommendation to go to five long-term campground rentals. All in favor, the motion carries.

B. Resolution 2024 – 11 2025 Preliminary Levy for Property Taxes due in 2025 – City Administrator

Motion: Lemke, seconded by Rivera to approve Resolution 2024-11 approving the 2025 Preliminary Levy for Property Taxes. Upon a roll call vote, the following voted Aye, Rivera, Olson, Hueser, Neid and Lemke. The following voted Nay, none. Whereupon the resolution was declared adopted and approved.

RESOLUTION NO. (2024-11)

RESOLUTION SETTING PRELIMINARY 2025 TAX LEVY

WHEREAS, the Department of Revenue has set September 30th, 2024 as the deadline for certifying 2025 Preliminary tax levies; and,

WHEREAS, the City Administrator has provided the City Council with the preliminary 2025 City General Fund and Debt Service Budgets, which includes a recommended Ad Valorem Tax Levy.

NOW THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF GLENCOE, MINNESOTA:

1. That the following sums of money be levied for the current year, collectable in 2025, upon taxable property in the City of Glencoe, for the following purposes:

<u>GENERAL</u>	
General Fund/Ad Valorem Levy	$1,787,000.00
<u>DEBT SERVICE/SPECIAL LEVY</u>	
Street Overlay	$ 800,000.00
2010 City Center	$ 160,000.00
2014 Street Improvement	$ 221,000.00
2015 Lincoln Park Project	$ 180,000.00
2016 Armstrong Ave Project	$ 37,000.00
2017 Baxter Avenue Project	$ 171,000.00
2018 Central Storm	$ 164,000.00
2021 10th Street Improvement	$ 25,320.00

Economic Development Authority	$ 125,000.00
	$1,883,320.00
TOTAL	$3,670,320.00

2. That the City Administrator is hereby instructed to transmit a certified copy of the levy to the County Auditor of McLeod County, Minnesota by September 30, 2024.
3. This is an increase over the 2024 tax levy.
4. That the Truth in Taxation hearing is set for December 2, 2024 at 7:15 p.m.; continuation hearing is set for December 16, 2024 at 7:00 p.m.

Adopted and approved this 18th day of September 2024.

_____

Ryan Voss

ATTEST: Mayor

_____

Mark D. Larson

City Administrator

8. ITEMS FOR DISCUSSION

A. Hotel/EDA Update – City Administrator
The Hotel Study has been finalized. We are currently setting up meetings with developers. Bryan Stading, our new EDA director will be present at the next EDA meeting virtually. We are working on setting up his office and hours of operation. His business cards have been delivered.

B. Revolve Labs update – City Attorney Ostlund
Bit 49 is manually being shut down every night to reduce sound. The new gate has been installed; the fence is still on back order. Looking at completing a new study end of Sept. beginning of Oct.

9. ROUTINE BUSINESS

A. Project Updates – Seal Coat project has been completed. All that is left to do is striping.
B. Economic Development
C. Public Input
D. Reports
E. City Bills

Motion: Neid, seconded by Lemke to pay the city bills. All in favor, the motion carries.

10. ADJOURNMENT

Motion: Lemke, seconded by Neid to adjourn the meeting. All in favor, the motion carries.

GLENCOE

SMALL CITY & BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

GLENCOE
SMALL CITY BIG FUTURE

City of Glencoe
Special Event Application
1107 11th Street East, Suite 107
Glencoe, MN 55336
320-864-5586
info@ci.glencoe.mn.us

Event name: Haunted Harvest at Oak Leaf Location: Oak Leaf Park - Shelters 1 & 2

Date(s) of the event: Oct. 18-19 and 25-26, 2024 Time(s) of event: 7-10pm

Group name or organization: Glencoe Days Contact Name: Myranda VanDamme

Address: 1107 11th St. E. Ste. 104 City: Glencoe Zip: 55336

Email: glencoedays@gmail.com Phone: 507-351-4433

Type of organization: For Profit ☐ Non-Profit ■ Charity ☐

Location requested: City Parking Lot ☐ City Park ■ Street Closure ☐

Estimated number of participants expected to attend the event: 300?

Event Description: Glencoe Days Haunted Harvest will included two haunted houses and a concession area. Our goal is to create another family friendly event for the community and area around that will included people of all ages.

Assistance Requested: Use of shelter 1 and 2. They will need to be used for the duration of the entire event so that equipment can be left up. The shelter will be closed for rentals already so no disturbance will be created. Parking in the park.

Street Closure Request - Describe the name and sections of the streets for requested closure.
N/A

Date/Time for beginning of street closure: _____

Date/Time for reopening of streets: _____

NOTE: Events using public streets and parking lots must submit a map with precise locations.

See back side for guidelines and agreement.

Special Event Guidelines

Special events include walk/runs, tournaments, concerts or gatherings of 50 participants or more in the City of Glencoe. Special Event Applications must be submitted at least 30 calendar days prior the event. Below is a list of additional items that may be required for your event, please review carefully.

Certificate of Liability Insurance: The City of Glencoe, at its discretion, may require the applicant to obtain a certificate of Liability Insurance. If required, applicants must provide a minimum of $1,000,000 of general liability coverage for each occurrence and shall name the City of Glencoe as an additional insured. Based on special event activities, some events may be required to obtain additional coverage. If you don't have private insurance or your organization does not have insurance, you may obtain insurance through the League of MN Cities Tenant User Liability Insurance Program (TULIP). Information on TULIP is located online at: www.lmc.org

Alcohol: If alcohol is sold or provided, the event must have proper licensing through State of MN and City of Glencoe. Liquor Liability Insurance is required for events that sell or provide alcohol.

Security: If the Chief of Police determines security is needed for the event, the organizer will be charged $100/hour per officer.

Street Closures: If a street closure occurs along residential streets, reasonable efforts must be made to alert all property owners along the street of the proposed closure. Failure to notify property owners in street closure areas or gain approval of street closures will result in revocation of permit.

Garbage: Organizers may be required to provide garbage containers and removal depending on the size of the event and the number of participants.

Sanitary Restrooms: Organizers may be required to provide sanitary restrooms depending on the size of the event and the number of participants.

Directional Markers: No paint or chalk paint should be used as directional markers on the trail systems in the parks or on the sidewalks and streets. Suggestions for directional markers include cones, sidewalk chalk, small signs or volunteers. Renter will be charged a fee if paint or permanent marks are placed on the trail system, sidewalks or streets. If you need cones or other materials from the Street Department, please make sure to include these items in the assistance requested section.

Contract Agreement: The renter will abide by all rules governed in City Ordinances and all City of Glencoe policies. The renter also understands that failure to abide by these rules and regulations could result in additional fees or denial of facility use.

_____ _____

Signature Date

City Staff Use Only Date Received: _____

Public Works Director ~~Street/Parks Recommendation~~: Approve ☑ Deny ☐

Comments: _____

Chief of Police Recommendation: Approve ☑ Deny ☐

Comments: _____

City Council: Approve ☐ Deny ☐ Date: _____

Updated: 5.20.2022

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 09/11/24

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Specialty Advantage Insurance Services
505 North Brand Blvd
Suite 1250
Glendale, CA 92103

CONTACT NAME: GatherGuard Administrator
PHONE (A/C, No, Ext): (844) 747-6240 **FAX (A/C, No):**
E-MAIL ADDRESS: gatherguard@intactinsurance.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A: Atlantic Specialty Insurance Company	27154
INSURER B:	
INSURER C:	
INSURER D:	
INSURER E:	
INSURER F:	

INSURED
Glencoe Days, Inc.
1107 11th St. E. Ste. 104
Glencoe, MN
55336

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY CLAIMS-MADE X OCCUR X Includes Host Liquor GEN'L AGGREGATE LIMIT APPLIES PER: X POLICY PROJECT LOC OTHER:	X		GGL041427	10/18/2024	10/27/2024	EACH OCCURRENCE	$ 1,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ Excluded
							PERSONAL & ADV INJURY	$ 1,000,000
							GENERAL AGGREGATE	$ 2,000,000
							PRODUCTS - COMP/OP AGG	$ 1,000,000
	AUTOMOBILE LIABILITY ANY AUTO OWNED AUTOS ONLY / SCHEDULED AUTOS HIRED AUTOS ONLY / NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident)	$
							BODILY INJURY (Per person)	$
							BODILY INJURY (Per accident)	$
							PROPERTY DAMAGE (Per accident)	$
								$
	UMBRELLA LIAB OCCUR EXCESS LIAB CLAIMS MADE DED RETENTION $						EACH OCCURRENCE	$
							AGGREGATE	$
								$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N ANY PROPRIETOR/PARTNER/EXECUTIVE/ OFFICER/MEMBER EXCLUDED? N/A (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A					PER STATUTE / OTH-ER	$
							E.L. EACH ACCIDENT	$
							E.L. DISEASE - EA EMPLOYEE	$
							E.L. DISEASE - POLICY LIMIT	$

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Event Name: Haunted Harvest at Oak Leaf
Event Type: Festival and cultural event (outdoors)
Event date(s): 10/18/24, 10/19/24, 10/25/24, 10/26/24
Daily Attendance: 300
Number of Days: 4

CERTIFICATE HOLDER

Oak Leaf Park
3 Desoto Avenue South
Glencoe, MN 55336 US

CANCELATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

GLENCOE

SMALL CITY BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

GLENCOE
SMALL CITY & BIG FUTURE

City of Glencoe
Special Event Application
1107 11th Street East, Suite 107
Glencoe, MN 55336
320-864-5586

Proposed event name: Customer Appreciation Event Proposed location: 1132 Hennepin Ave N

Date(s) of the event: Tuesday October 15th Time(s) of event: 8 - 11 am

Group name or organization: JL Insurance Advisors Contact Name: Cadee Winnie

Address: 1132 Hennepin Ave N City: Gelncoe Zip: 55336

Email: cadeewinnie@aibme.com Phone: 320-864-3943

Type of organization: ○ For Profit ○ Non-Profit ○ Charity

Location requested use: ○ City Parking Lot ○ City Park ◉ Street Closure

Estimate the number of participants you expect to attend the event: est 100 pp +

Event Description: We are hosting a customer appreciation - meet and greet event at our office - and Ribbon Cutting with the Chamber of Commercce. We will have Elephant Joes coffee truck and serving mini donuts.

Assistance Requested: would like picnic tables and barricades of some sort to keep people safe with in the parking spots

Street Closure Request:
Describe the name and sections of the streets you are requesting temporary closure:
Parking spaces against our office location on 12th street

Date/Time for beginning of street closure: Tuesday Oct 15th 7 am

Date/Time for reopening of streets: Tuesday October 15th 12 pm

Events using public streets and parking lots (parades, walk/runs, dances, etc.) must submit a map with precise locations.

See back side for guidelines and information.

Guidelines for Special Events

City of Glencoe Special Events
Special Event Permits are required to conduct special events. Special events include walk/runs, tournaments, concerts or gatherings of 50 participants or more in the City of Glencoe. Special Event Applications must be completed at least 30 calendar days prior the event. Below is a list of additional items that may be required for your event, please review carefully.

Certificate of Liability Insurance: The City of Glencoe, at its discretion, may require the applicant to obtain certificate of Liability Ins to host a special event. If required, applicants must provide a minimum of $1,000,000 of general liability coverage for each occurrence and shall name the City of Glencoe as an additional insured. Based on special event activities, some events may be required to obtain additional coverage. Contact your organization or private insurance company to obtain liability insurance. If you don't have private insurance or your organization does not have insurance, you may obtain insurance through the League of MN Cities Tenant User Liability Insurance Program (TULIP). Information on TULIP is located online at: http://www.lmc.org/page/1/Tenant-User-Liability-Insurance-Program.jsp.

Alcohol: If alcohol is sold or provided, the event must have proper licensing through State of MN and City of Glencoe. Liquor Liability Insurance is required for events that sell or provide alcohol.

Street Closures: All street closures must be approved by Chief of Police. If a street closure occurs along residential streets, reasonable efforts must be made to alert all property owners along the street of the proposed closure. Failure to notify property owners in street closure areas or gain approval of street closures will result in revocation of this permit.

Garbage: Depending on the size of the event and the number of participants may be required to provide own garbage containers and pick up.

Sanitary Restrooms: Depending on the size of the event and the number of participants may be required to provide own sanitary restrooms.

Directional Markers: No paint or chalk paint should be used as directional markers on the trail systems in the parks or on the sidewalks and streets. Suggestions for directional markers include cones, sidewalk chalk, small signs or volunteers. Renter will be charged a fee if paint or permanent marks are placed on the trail system, sidewalks or streets. If you need cones or other materials from the Street Department, please make sure to include these items in the assistance requested section.

Contract Agreement: The renter will abide by all rules governed in City Ordinances and all City of Glencoe Department policies. The renter also understands that failure to abide by these rules and regulations could result in additional fees or denial of facility use.

Cadee Winnie — Signature

09.27.2024 — Date

City Staff Use Only Date Received: _____

Public Works Director Street/Parks Recommendation: Approve ☑ Deny ☐
Comments: City staff will place barricades & cones out at 7:30 am and remove at 12pm. picnic table will be dropped of at 8am

Chief of Police Recommendation: Approve ☑ Deny ☐
Comments: Barricades will be needed to protect people sitting on 12th St. in park spaces

City Council: Approve ☐ Deny ☐ Date: _____

Tony Padilla

From: cadeewinnie@aibme.com
Sent: Tuesday, October 1, 2024 11:25 AM
To: Tony Padilla; Haylie Kusler
Subject: Re: Request
Attachments: Screenshot 2024-10-01 112019.png

Yellow Area on the north side of the building - EVENT AREA

Blue Hashes - PARKING SPOTS

Would like barricades at the end of the parking spaces - Picnic tables will be placed with in the Parking spots off the road way.

Shouldn't have to shut down any roads unless you want to shut off 12th street from Hennepin Ave to the end of our Building / alley Before Alseben Meats.

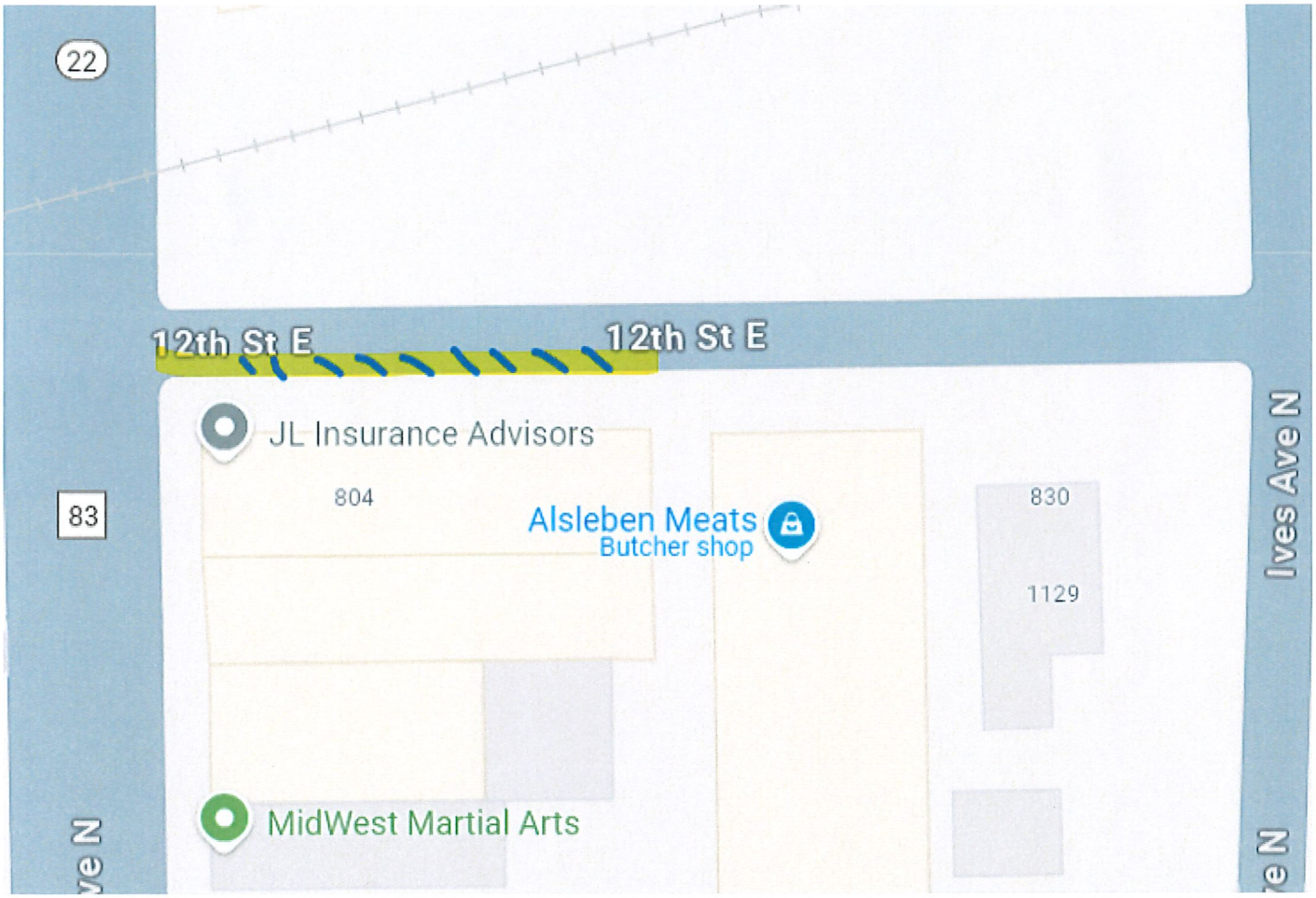
Cadee Winnie, *Agency Owner*
Atlas Insurance Brokers, LLC - JL Insurance Advisors
1132 Hennepin Ave N, Glencoe, MN 55336
Ph: (320) 864-3943 **Text:** (320) 348-7528
cadeewinnie@aibme.com | www.jlinsurancemn.com

JL INSURANCE
ADVISORS

Receive a $20 gift card for qualified referrals!

From: Tony Padilla <tpadilla@ci.glencoe.mn.us>
Sent: Monday, September 30, 2024 3:44 PM
To: cadeewinnie@aibme.com <cadeewinnie@aibme.com>; Haylie Kusler <hkusler@ci.glencoe.mn.us>
Subject: RE: Request

Hello,


22
12th St E
12th St E
JL Insurance Advisors
804
Alsleben Meats
Butcher shop
830
1129
83
Ives Ave N
MidWest Martial Arts

GLENCOE
SMALL CITY & BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

GLENCOE

SMALL CITY BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

To: Mayor and City Council

From: Mark Lemen, Assistant City Administrator/Public Works Director

Date: October 7, 2024

RE: **Item 7A** - Proud FFA Community Signs

Item 7A - Last week, MNDOT approved a permit for the local FFA chapter to hang signs stating that Glencoe is a "Proud FFA Community" on the City population signs on Highways 212 and 22. The City Street/Park department will install the signs this week.

The FFA chapter is present at the Council meeting tonight to present the information to the City Council and express their appreciation for the City's cooperation with this project.

Mark Larson

From: Liz Griebel
Sent: Wednesday, October 2, 2024 3:07 PM
To: Mark Larson; Mark Lemen; Jamie Voigt
Subject: Re: FFA Community Signs

We received the approved permit from MNDoT for the FFA signs to be placed on the city population signs on 212 and 22. They have indicated the next step is for city approval and either the city staff or the group (FFA) to install them.

How do we go about getting city approval and getting them installed?

Liz Griebel
Glencoe Aquatic Center Director
City of Glencoe
952-847-0263 (cell)
320-864-2959 (pool office)

From: Mark Larson <mlarson@ci.glencoe.mn.us>
Sent: Thursday, September 5, 2024 1:16 PM
To: Liz Griebel <ltromborg@ci.glencoe.mn.us>
Cc: Mark Lemen <MLemen@ci.glencoe.mn.us>; Cody Brand <cody.brand@state.mn.us>
Subject: Re: FFA Community Signs

Liz,

I think that Cody with MNDOT can help you. I have copied him on this email.

Cody Brand, P.E.
Traffic Engineer | District 8
Cell Phone (320) 979-4720

Sent from my iPhone

> On Sep 5, 2024, at 11:24 AM, Liz Griebel <ltromborg@ci.glencoe.mn.us> wrote:
>
> Good morning!
>
> The Glencoe-Silver Lake FFA chapter is seeking contact information to receive approval for having the Proud FFA Community signs posted on various roads throughout the school district.
>
> #1 - Glencoe US Highway 212

GLENCOE
SMALL CITY & BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

Item 7B

Glencoe Police Department

Memo

To: Glencoe City Council

From: Tony Padilla- Chief of Police

cc:

Date: September 25, 2024

Re: Update GPD Policy 1.21 Section A CJIS Security Policy

Glencoe Police Department (GPD) recently went through a mandatory State Bureau of Criminal Apprehension (BCA) security audit. During the audit our security policy was updated. The policy attached to this memo has all the updates highlighted in yellow that were added since receiving the BCA audit in September 2024.

GLENCOE POLICE DEPARTMENT
POLICIES /RULES/PROCEDURES

POLICY NUMBER: **1.21 section A**

POLICY TITLE: **CJIS SECURITY POLICY**

SECTION:

PURPOSE:

The purpose of this policy is to provide an aggregate collection of standards, controls and requirements necessary to ensure full compliance with the FBI Criminal Justice Information Services Security Policy for accessing CJIS information and services consistent with all applicable laws, executive orders, directives, policies, regulations, standards, and guidance.

POLICY:

DEFINITIONS

Access – Creation, viewing, modification, transmission, dissemination, storage or destruction of any electronic data on any system, device or network connection which may have CJIS data.

Authorized Agency – A government Agency authorized by the BCA to have access to BCA and FBI resources and that has a valid joint powers agreement or other contact executed by it and the BCA.

BCA – Bureau of Criminal Apprehension (the CJIS Systems Agency CSA and State Identification Bureau SIB) for Minnesota.

Certificate Authority (CA) - Certificate Authority is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. This includes centralized, automated systems such as card management systems.

Certificate Revocation List (CRL) - A list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.

Criminal Justice Data Communications Network (CJDN) - For statutorily authorized users, the CJDN is a connectivity method that has been approved by the BCA.

Criminal Justice Environment (CJE) - An authorized Agency's isolated infrastructure where CJI passes is accessed, and/or stored. This includes, but is not limited to, network switches, routers, firewalls, workstations, servers, and virtual environments.

Criminal Justice Information (CJI) or Data - Any criminal justice information, as defined in Section 4 of the FBI CJIS Security Policy, whether complete or in part, regardless of content or application, stored or transmitted on a system. Criminal Justice Information is the abstract term used to refer to all data from systems containing, integrated with or derived from data in the FBI CJIS repositories and also includes data contained in, integrated with or derived from data maintained in BCA repositories and that are necessary for authorized agencies to perform their work.

Criminal Justice Information System (CJIS)

CJIS Systems Officer (CSO) - CJIS Systems Officer is the BCA employee responsible for the administration of the system that makes it possible to send and retrieve CJI.

Degaussing - A method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degaussers. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

Electronic/Digital Media - Any medium that can and store digital data such as hard drives, random access memory (RAM), read-only memory (ROM), magnetic tape or disk, memory card devices and many other types listed in Appendix A of NIST 800-88.

Federal Bureau of Investigations (FBI)

Federal Information Processing Standard (FIPS)

Information System - A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Information System Authenticators - Information system authenticators include, but not limited to, tokens, user based PKI certificates, biometrics, passwords, smart cards, and keycards.

Information Security Officer (ISO)

Local Area Security Officer (LASO)

Limited Function Devices - Any operating systems such as iOS, Android, and Windows Mobile, or any other version of *nix, Windows Operating Systems that have been streamlined and or hamstrung to reduce base operating system capability.

Local Agency - Any Minnesota Agency, including federal agencies that serve part or all of Minnesota, authorized to access the CJDN.

MNJIS Terminal - Any device used by a Local Agency to connect to the CJDN to retrieve CJI. Examples of a MNJIS Terminal include, but are not limited to, a desktop computer, laptop, tablet, and cellular telephone.

Minnesota Justice Information Services (MNJIS)

Mobile Device - Any portable device used to access CJI via a wireless connection. Examples of mobile devices are smart phones, cellular phones transmitting CJI, laptops and tablets and other portable equipment, which can easily be moved from one location to another.

National Institute of Standards and Technology (NIST) - A measurement standards laboratory and a non-regulatory Agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

Online Certificate Status Protocol (OCSP) - an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

Personally Identifiable Information (PII) - Information which can be used to distinguish an individual's identity, alone or combined with other personal or identifying information, which is linked or linkable to as individual, such as date and place of birth, or mother's maiden name. Qualifying items include: Name, Social Security Numbers, Taxpayer Identification Numbers, Employer Identification Numbers, State or foreign driver's license numbers, Date(s) of birth, Corporate or individually held credit or debit transaction card numbers (including PIN or access numbers) or biometric records.

Personally Owned Devices - Any device not issued or purchased by the Agency; this includes and not limited to USB flash storage, flash storage, mobile phones, laptops, or any other electronic device capable of storing CJI.

Physically Secure Location - A facility, area, room, or a group of rooms that have the physical and personnel security controls sufficient to protect CJI and the associated information system.

Physical Media - Printed document(s) or any electronic device which stores information.

Public Key Infrastructure (PKI) - Algorithms and encryption that use key pairs to secure CJI whether in transit or at rest.

Registration Authorities (RA) - Collect and verify each subscriber's identity and information that is to be entered into the subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by the Policy Authority.

Remote - Outside of a secure facility for this document and connecting to a criminal justice network through a wireless connection.

Virtual Machines (VM) – In computing, a virtual machine (VM) is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.

Wi-Fi Protected Access (WPA) - Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP).
WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

Wired Equivalent Privacy (WEP) - A security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

Wireless Technology – Transmission of voice and/or data communications via radio frequencies.

This policy applies to all Glencoe Police Departments, employees, contractors, temporary staff, and other workers at Glencoe Police Department with access to LEIN/NCIC CJIS systems and/or data, sensitive and classified data, and media. This policy applies to all systems that may have access to criminal justice information that process, store, and/or transmit LEIN/NCIC CJI and classified and sensitive data owned or leased by Glencoe Police Department.

Relationship to Local Security Policy and Other Policies
Reference: FBI CJIS Security Policy 1.3

This document is a compendium of applicable policies providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions.

Unless explicitly stated in this document the FBI CJIS Security Policy acts as the standard security policy for Glencoe Police Department when criminal justice information is involved. The Glencoe Police Department CJIS Security Policy shall meet the minimum standards of the FBI CJIS and BCA MNJIS 5002 Security Policies; however a more restrictive policy may be set should business and or mission needs justify and/or require.

Glencoe Police Department shall work on an ongoing basis to ensure this policy and any associated operational procedures align with the current overarching FBI CJIS Security Policy. Glencoe Police Department has a copy of the new FBI CJIS Security Policy v5.6 (5 Jun2017) and shall maintain written procedures of actions implemented for review, upon request.

Personally Identifiable Information (PII)
Reference: FBI CJIS Security Policy 4.3

- PII may reside in hard copy or electronic records; both forms of PII shall fall within the scope of this policy.

- Glencoe Police Department recognizes its need to maintain the confidentiality of Personal Identity Information (PII) and understands that such information is unique to each individual and such shall protect data that is collected and stored on individuals. Where necessary, information that is stored shall be safeguarded and secured to protect against data breaches and/or leaks.
- Glencoe Police Department shall revise its policy, on an ongoing basis, to ensure alignment with state and local privacy rules and appropriate controls are applied when handling PII.
- Departments shall have delegated authority for developing and implementing procedural guidance for ensuring that their departmental responsibilities under this policy are communicated and enforced.
- All electronic or physical data containing PII shall be protected from unauthorized disclosure or access to the same or greater level than CJI.
- PII shall be extracted from CJI for the purpose of official business only.
- Appropriate parties shall be informed of unintentional disclosure or breach in a timely fashion or as required by governing local, state or federal laws.
- All state and local privacy rules shall be complied with, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, disclosure or personnel security requirements associated with the life cycle of PII.
- **Vendors**
    - Vendors include all external providers of services to Glencoe Police Department and include proposed vendors.
    - Individual(s) or companies must be approved for access to organizational PII. Approval requires receipt of certification documenting that their data protection practices are in conformance with all requirements of this policy.
    - No PII information can be transmitted to any vendor in any method unless the vendor has been approved.
- **PII Retention**
    - Glencoe Police Department understands the importance of minimizing the amount of PII data it maintains and retains such PII only as long as necessary.
    - The Glencoe (City) Attorney's Office shall maintain a record of organizational retention procedures, which dictate the length of data retention and data destruction methods for both hard copy and electronic records.
- **PII Training**
    - All new hires at Glencoe Police Department who may have access to PII shall be provided with introductory training regarding the provisions of this policy, a copy of this policy and implementing procedures for the department to which they are assigned.
    - Employees in positions with regular ongoing access to PII or those transferred into such positions shall be provided with training reinforcing this policy and procedures for the

maintenance of PII data and shall receive annual training regarding the security and protection of PII data and City proprietary data.

- **PII Audit(s)**
    - Glencoe Police Department shall conduct audits of PII information maintained by Glencoe Police Department in conjunction with fiscal year closing activities, to ensure that this policy remains strictly enforced and to ascertain the necessity for the continued retention of PII information.
    - PII information shall be destroyed in accordance with protocols for destruction of such records. Logs shall be maintained for the dates of destruction, where a need for retention no longer exists.
- **Data Breaches/Notification**
    - Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, all affected individuals whose PII data may have been compromised shall be notified, and the notice shall be accompanied by a description of action being taken to reconcile any damage because of the data breach.
    - Notices shall be provided as expeditiously as possible and in no event be later than the commencement of the payroll period after which the breach was discovered.
    - The Glencoe (City) Attorney's shall handle breach notifications(s) to all governmental agencies to whom such notice must be provided, in accordance with periods specified under these laws.
- **Data Access**
    - Glencoe Police Department maintains multiple systems where PII data may reside.
        - User access at the application level is the responsibility of the department owning and administering each specific system.
        - User access to the network and file shares/containers/directories is technically administered by the Cities IT Support and implemented in accordance with formal requests from individuals having ownership or responsibility over those information repositories.
    - The Cities IT Support has created internal controls to establish legitimate access for users of data. Access shall be limited to those approved and formally requested by individuals having ownership or responsibility over each relevant application and information repository.
    - Any change in vendor status or the termination of an employee or independent contractor with access shall result in the timely termination of that user's access to all systems where the PII may reside.

Data Transmission and Transportation

- **Glencoe Police Department Premises Access to PII**

- Glencoe Police Department has defined responsibilities for on-site access of data that may include access to PII. The Cities IT Support has the oversight responsibility for all electronic records and data access capabilities.
- Glencoe Police Department has the operational responsibility for designating initial access and termination of access for individual users, with Human Resources providing timely notice to Department of Information Systems.

- **Vendors**
  - Data may be shared with vendors who have a business need to have PII data. Where such inter/Agency sharing of data is required, the Cities IT Support is responsible for creating and maintaining data encryption and protection standards to safeguard all PII data that resides in the databases provided to vendors.
  - Approved vendor lists shall be maintained by Glencoe Police Department and shall be the responsibility of that departments to notify City's IT Support of any changes to vendor status with Glencoe Police Department.
- **Portable Storage Devices**
  - Glencoe Police Department reserves the right to restrict PII data it maintains in the workplace.
  - To facilitate business operations, PII data may be downloaded to laptops or other computing storage devices. To protect such data, Glencoe Police Department shall require that any such devices use City's IT Support approved encryption and security protection software while such devices are in use, whether on or off City premises.
  - The City's IT Support has responsibility for maintaining data encryption and data protection standards to safeguard PII data that resides on these portable storage devices.
- **Off-Site Access to PII**
  - Employees may need to access PII while off site or on business travel. Access to such data shall be allowed if the data accessed is minimized to the greatest extent possible, sufficient to meet business operational needs. Such data shall reside only on assigned laptops/approved storage devices that have been secured in advance by the Department of Information Systems.
- **Regulatory Requirements**
  - Glencoe Police Department shall maintain compliance with any federal or state statute, as well as reporting regulations to which is subject.
  - Glencoe Police Department has delegated the responsibility for maintaining PII security provisions to City departments.
  - The Glencoe (City) Attorney's Office shall be the sole entity named to oversee all regulatory reporting compliance issues.

- If any provision of this policy conflicts with a statutory requirement of international, federal or state law governing PII, the policy provision(s) that conflict shall be superseded.

- **Compliance Hotline**
  - If an employee has reason to believe that PII data security has been breached or that City representative(s) are not adhering to the provisions of this policy, an employee should contact the Police Chief.

- **Confirmation of Confidentiality**
  - All Glencoe Police Department employees must maintain the confidentiality of PII as well as City proprietary data to which they may have access and understand that that such PII is to be restricted to only those with a business need to know.
  - Employees with ongoing access to such data shall sign acknowledgement reminders annually attesting to their understanding of this Glencoe Police Department requirement.

Information Exchange
Reference: FBI CJIS Security Policy 5.1.1

Glencoe Police Department has Management Control Agreements in place with the Sheriff's Office and City Attorney's Office. Joint Powers Agreements are in place with local agencies who share information with Glencoe Police Department.

- CJI, whether in part or complete, shall be used for official business purposes only and only by personnel required to fulfill their specific position duties. When required by federal, state, or local regulations, data access shall be logged.
- Release or exchange of CJI to non-authorized Agency(s) or individual is strictly prohibited.
- Individuals shall verify that the recipient is an authorized individual prior to exchange.
- The Agency shall maintain control of authorized use.
- Information Exchange Agreements shall outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.
- LASO shall ensure that formal agreements that specify security controls are in place prior to exchange of CJI physically or electronically.
- When releasing or sharing CJI with another authorized Agency or individual, a log shall be maintained.
- Releasing digital CJI to another authorized Agency or individual shall only be done using appropriate digital media, as defined in this policy.
- Logs of exchange of CJI to an authorized Agency or party, physical or electronic, shall be maintained for a minimum of a year (365 days).

- Transferring CJI electronically through email, FTP, cloud services, internet protocols, or similar means is strictly prohibited. While these methods can be designed and approved to transport CJI, Glencoe Police Department does not have these methods or procedures defined at this time. This does not include access CJI through authorized internet applications.

Information Handling
Reference: FBI CJIS Security Policy 5.1.1.1

- All information received directly or indirectly from the BCA and its resources shall be classified as CJI and as such shall be protected with full compliance to CJIS and BCA security requirements.
- All users with access shall be familiar and shall take measure to protect CJI while handling, processing, storing, and communicating any CJI.
- All users with unescorted access, as well as Glencoe Police Department staff, who come in direct or indirect contact with CJI information, shall sign Acceptable Use Policy in recognition to project CJI.
- These procedures shall apply to the exchange of CJI no matter the form of exchange.
- Any violations shall be reported to the LASO. The LASO shall report violations to the BCA ISO office.
- All Glencoe Police Department users who access CJI shall have the training necessary to ensure compliance and follow all policies related to the handling of this information.

The Agency and City's IT Support shall protect CJI and subsets of CJI by adhering to the following procedures:

- Securely store electronic and physical media within a physically secure or controlled area.
- Restrict access to electronic and physical media to authorized individuals.
- Ensure that only authorized users remove printed form or digital media.
- Physically protect media end of life.
- Ensure end of life media is destroyed or sanitized.
- Use only City owned/provided information systems to access, process, store, or transmit CJI Not utilize publicly accessible computers to access, process, store, or transmit CJI.
- Store all hardcopy CJI printouts maintained in a secure area accessible to only those employees whose job function require them to handle such documents.
- Safeguard all media against possible misuse by complying with all other applicable Glencoe Police Department or department specific policies.
- Media at rest (stored electronically) outside the boundary of the physically secure location shall be protected using encryption certified to meet FIPS 140-2 standards.

- Users shall be required to lock or log off computer when not in immediate vicinity of work area, to protect access.

Incident Response
Reference: FBI CJIS Security Policy 5.3

The security risk of both accidental and malicious attacks against government and private agencies remains persistent in both physical and logical environments.

- In the event of an accidental or malicious information system security incident, the Agency and City's IT Support shall work together to properly mitigate the risk of CJI access.
- Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken.
- Formal event reporting and escalation procedures shall be in place. Wherever feasible, automated mechanisms shall be employed to assist in the reporting of security incidents.
- Upon suspicion of a compromised system, Department of Information Systems, the Agency, or the individual shall immediately disconnect the system from the rest of the network. Once free from infection the system can be reconnected.
- All employees, contractors and third party users shall be made aware of procedures for reporting the different types of event and weakness that might have an impact on security and are required to report any security events and weaknesses as quickly as possible to the LASO.
- LASO is to be the primary point of contact for interfacing with the CSA/BCA concerning incident handling and response.
- LASO shall report security incident information within 24 hours of discovery to BCA/ISO to include a security incident form as found in CJIS Security Policy.
- LASO shall collect incident information from individuals for coordination and notify appropriate stakeholders.

  LASO shall develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.

- LASO shall collect and disseminate all incident-related information to bca.iso@state.mn.us with Security Incident Form as found in Appendix H of CJIS Security Policy.
- LASO shall act as a single POC for their jurisdictional area for requesting incident response assistance.
- The City's IT Support shall maintain all records around information security events at both the network and operating system levels.
- Information to be collected on Incident Response Form shall include:
- Suspected cause for incident
- Identification of security software running at the time of infection
- How and when the problem was first identified

- When City's IT Support were notified
- Number and types of systems infected
- If a mobile device was lost, stolen or compromised:
    - Was the device known to be locked?
    - Was the device outside of the United States?
    - Action plan for removal
    - Specification whether CJIS data or PII were compromised

Access Control
Reference: FBI CJIS Security Policy 5.5.2.2(1)

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.

- Access controls shall be in place and operational on all Agency Information Systems.
- Only authorized users shall be granted access to CJIS, and users shall be limited to specific defined, documented and approved applications and levels of access rights.
- Each user shall be uniquely identified and shall not have shared access to CJIS. This is to provide nonrepudiation for all logged or log-able activity.
- Multiple concurrent active sessions shall not be allowed for one user identification, unless authorized in writing for a limited time by LASO or Chief on a case-by-case scenario.
- This policy applies to all who have physical and logical access to CJI information systems.
- Any user accessing Agency resources shall be authenticated in compliance with FBI CJIS Security Policy with the following control measures at a minimum: Automatic Logoff, Automatic Lock, and at least one of the following: Password, PIN, or Advanced Authentication (if outside of secure area)
- All Agency information systems shall be protected and kept secure.
- User shall log off information system when left unattended for a prolonged period, where appropriate. The user shall be held responsible for all actions taken under their sign-on.
- User shall be required to re-authenticate after screen lock.
- Screen lock shall not be disabled or circumvented by the user or any other party.
- A notice warning that those should only access the system with proper authority shall be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and those unauthorized users should disconnect or log off immediately.
- System access shall not be granted to any user without appropriate approval and clearance.
    - Management/supervisor is to immediately notify LASO and report all significant changes in end user duties or employment status.

- User access is to be immediately revoked if the individual has been terminated.
- User privileges are to be appropriately changed if the user is transferred to a different job.

- Agency approved access controls, such as user login scripts, menus, session managers, and other access controls shall be used to limit access to only those network applications and functions for which users have been authorized to access.
- Users shall be granted access to information on a "need-to know" basis. That is, users shall only receive access to the minimum applications and privileges required performing their jobs.
- All users who have access to CJI shall sign and agree to the terms in the Acceptable Use Policy and other relevant policies that govern the use and access of CJE.
- All users shall review, confirm, and agree to abide by the policies that govern the use of Agency's information systems.
- Agency and the City's IT Support shall review this policy bi-annually to ensure Agency shall address new technology and threats.
- Passwords:
  - Shall meet or exceed CJIS Security Policy requirements.
  - Shall be reviewed regularly to disable inactive accounts.
  - Shall not be stored or transmitted in a readable form.
  - Shall not be displayed and shall be obscured such that it may not be recovered.
  - Shall be utilized by all applications, programs, and devices supporting use.
  - Shall be forced to change (or manually be required to be changed) at intervals of at least every ninety (90) days.
  - All unnecessary operating system or application users IDs and passwords not assigned to an individual user shall be deleted or disabled.
  - In case of multiple consecutive authentication failures, systems shall lock the account until a system administrator unlocks the account.
- Shared resources shall be partitioned according to business needs and access shall be limited to only necessary personnel.
- Supervisors shall notify City's IT Support of changes in staff as soon as they happen, or at the earliest possible time. This includes hires, leaves, terminations, etc.
- Users account shall be immediately disabled/changed as soon as notified, or at the earliest possible time.
- LASO and System Administrator shall review accounts at a minimum of every six (6) months.
- LASO and System Administrator shall verify that security measures are in fact working, and remediate any deviations.

- LASO and System Administrator shall receive notifications of locked accounts on a regular basis.
- LASO and System Administrator shall test implemented security measures at a minimum of every six (6) months.
- LASO and System Administrator shall review security logs when notifications are received through monitoring system.
- Only authorized personnel shall add, change, or remove component devices, install, remove or alter programs and can only be done when necessary for business purposes. System Access Control must comply with Section 5.5.2.2 of the FBI CJIS Security Policy.

Remote Access
Reference: FBI CJIS Security Policy 5.5.6

- It is the responsibility of Agency employees, contractors, vendors and agents with remote access privileges to Agency's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Agency.
- The system shall implement VPN mechanisms using technologies such as data encryption, key management, access control, authentication, and data integrity.
- The system shall utilize cryptographic modules that are compliant with Federal Information Processing System (FIPS) Publication 140-2 for Security Requirements for Cryptographic Modules.
- At a minimum, a user shall be restricted from establishing a VPN session without first being identified/authenticated by an advanced authentication method (minimum of 2-factor authentication). Identification/authentication can take place at the network, device, application, and/or device/software levels.
- LASO is responsible for enforcing a timeout on all VPN sessions.
- LASO shall log/maintain/review remote privileged accounts and disable unnecessary accounts.
- LASO may approve Remote access with elevated privileges to meet specific needs for a limited time. Such situations shall be documented by LASO with routine review of the logs by the Systems Administrator.
- Mobile devices or workstations shall be protected with City's IT Support approved malware prevention/security software.
- All hosts that are connected to City networks via remote access technologies must use the most up-to date malware prevention software and definitions.
- All remote, Glencoe Police Department-issued equipment must be configured with the minimum supported operating system installed and firewall-enabled or other City's IT Support approved software or hardware firewall.
- At no time shall any city employee provide his or her VPN login to anyone.

- Employees and contractors with remote access privileges shall ensure that computers or devices being used to remotely connect to the Glencoe Police Department network are not connected to any other network at the same time. Reconfiguration of equipment for split-tunneling or dual homing is not permitted.
- Employees and contractors with remote access privileges to the Glencoe Police Department network must not use non-city email accounts (i.e., Hotmail, Yahoo, Gmail, etc.), or other external resources for City business purposes.
- All hardware configurations are to be approved by the LASO and they must approve security configurations for access to hardware.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the Glencoe Police Department network must obtain prior approval from the LASO.
- Glencoe Police Department shall authorize, monitor, and control all methods of remote access to the identified system.
- Glencoe Police Department shall employ automated mechanisms to facilitate the monitoring and control of remote access methods.
- Glencoe Police Department shall control all remote accesses through managed access control points.
- Glencoe Police Department shall require advanced authentication when required.

Personally Owned Information Systems
Reference: FBI CJIS Security Policy 5.5.6.1

A personally owned information system shall not be used to access, process, store or transmit CJI unless the Agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices are authorized, they shall be controlled in accordance with the requirements set forth in policy section "Mobile Devices."

This control does not apply to the use of personally owned information systems to access Agency's information systems and information that are intended for public access (e.g., an Agency's public website that contains purely public information).

Authentication Policy and Procedures
Reference: FBI CJIS Security Policy 5.6.2

- Each individual's identity shall where possible be authenticated on the Glencoe Police Department Domain and not on the local device or information system.
- Individuals shall have a unique user ID, which shall be required each log in attempt. The previous logged in user ID will not be visible and must be entered at each log in attempt.
- Five (5) invalid login attempts shall result in an automated account lockout.
- Minimum complexity of password, PIN, Pass Phrase and duration of validity shall be:
    - Passwords

        - Shall be a minimum of sixteen (8) characters long.
        - Shall not be a dictionary word or name.
        - Shall have at least one (1) capital letter.
        - Shall have at least one (1) special character.
        - Shall not be the same as user ID.
        - Shall not be valid longer than ninety (90) days.
        - Shall not be same for the past ten (10) passwords.
    - PIN
        - Shall be a minimum of six (6) numbers.
        - Shall not use repeating numbers.
        - Shall not use ascending/descending numbers.
        - Shall be valid for three-hundred and sixty five (365) days.
        - Shall not be same for the past ten (10) PINs.

  The authentication strategy shall be part of the Agency's audit for policy compliance.
    - Authentication shall not be displayed while entering.
    - Authentication shall not be sent in the clear.
    - Authentication shall be encrypted.
- Advanced authentication and approved encryption shall be used when user is utilizing a wireless network or authenticating from an unsecured location or police conveyance.
- Passwords, pass phrase, and PIN shall not be written, recorded or shared.
- LASO shall ensure that System Administrators employ technical measures to ensure authentication compliance and test the system periodically.
- In an event of lost/stolen authentication credentials, individual shall notify the LASO immediately.

Authenticator Management
Reference: FBI CJIS Security Policy 5.6.3.2.2(2)

City authenticators include passwords, electronic lock key cards, and VPN token fobs.
- Users shall make all reasonable attempt to keep the authenticator secured. Users shall not leave it unsecured in a vehicle.
- Authenticator shall not be shared or loaned.
- Lost authenticator shall be reported in a timely fashion to supervisor and to the LASO.
- LASO shall terminate access with the lost authenticator as expediently as possible.

- Glencoe Police Department requires all staff to notify City's IT Support immediately of any lost or stolen authenticators. Users must safeguard this data and never leave it unattended.
- Glencoe Police Department City's IT Support is responsible for distribution and revocation of authenticators and maintaining a list of this access.

Media Protection
Reference: FBI CJIS Security Policy 5.8

Media Protection is necessary to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules. Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Media Access:

- Through the direction from the Glencoe Police Department City's IT Support shall restrict access to digital and non-digital media to authorized individuals.
- Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.

Media Storage:

- The Glencoe Police Department shall physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible.
- Protect system media types defined in media access until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Media Transport:

- The Glencoe Police Department shall protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel.
- Maintain accountability for system media during transport outside of the physically secure location or controlled areas.
- Document activities associated with the transport of system media.
- Restrict the activities associated with the transport of system media to authorized personnel.

Media Sanitization:

- The Glencoe Police Department shall sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration.
- Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Media Use:

- The Glencoe Police Department shall restrict the use of digital and non-digital media on Glencoe Police Department owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls.
- Prohibit the use of personally owned digital media devices on all Glencoe Police Department owned or controlled systems that store, process, or transmit criminal justice information.
- Prohibit the use of digital media devices on all Glencoe Police Department owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.

Physical Protection
Reference: FBI CJIS Security Policy 5.9

Glencoe Police Department and the City's IT Support recognizes the need for securing the information and information systems that contain CJI. To ensure that resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

Physical Access Authorizations:

- The Glencoe Police Department shall develop, approve, and maintain a list of individuals with authorized access to Glencoe Police Department where the system resides.
- Issue authorization credentials for Glencoe Police Department access.
- Review the access list detailing authorized Glencoe Police Department access by individuals annually and when personnel changes occur.
- Remove individuals from the Glencoe Police Department access list when access is no longer required.

Physical Access Control:

- The Glencoe Police Department shall enforce physical access authorization by:
    - Verifying individual access authorizations before granting access to Glencoe Police Department.

    - Controlling ingress and egress to Glencoe Police Department using agency-implemented procedures and controls.
- Maintain physical access audit logs for the Glencoe Police Department and agency-defined sensitive areas.
- Control access to areas within the Glencoe Police Department designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers.
- Escort visitors and control visitor activity in all physically secure locations of the Glencoe Police Department.
- Secure keys, combinations, and other physical access devices.
- Inventory all agency-issued physical access devices annually.
- Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

Access Control for Transmission:

- The Glencoe Police Department shall control physical access to information system distribution and transmission lines and devices within the Glencoe Police Department facilities using agency-implemented procedures and controls.

Access Control for Output Devices:

- The Glencoe Police Department shall control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.

Monitoring Physical Access:

- The Glencoe Police Department shall monitor physical access to the Glencoe Police Department where the system resides to detect and respond to physical security incidents.
- Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI.
- Coordinate results of reviews and investigations with the Glencoe Police Department incident response capability.
- Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Visitor Access Records:

- The Glencoe Police Department shall maintain visitor access records to the Glencoe Police Department where the information system resides for one year.
- Review visitor access records quarterly.
- Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.

- Limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected.

Power Equipment and Cabling:

- The Glencoe Police Department shall protect power equipment and power cabling for the system from damage and destruction.

Emergency Shutoff:

- The Glencoe Police Department shall provide the capability of shutting off power to all information systems in emergency situations.
- Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel.
- Protect emergency power shutoff capability from unauthorized activation.

Emergency Power:

- The Glencoe Police Department shall provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.

Emergency Lighting:

- The Glencoe Police Department shall employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Fire Protection:

- The Glencoe Police Department shall employ and maintain fire suppression and detection systems that are supported by an independent energy source.
- Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.

Environmental Controls:

- The Glencoe Police Department shall maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels.
- Monitor environment control levels continuously.

Water Damage Protection:

- The Glencoe Police Department shall protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Delivery and Removal:

- The Glencoe Police Department shall authorize and control information system-related components entering and exiting the Glencoe Police Department.

- Maintain records of the system components.

Alternate Work Site:

- The Glencoe Police Department shall determine and document all alternate facilities or locations allowed for use by employees.
- Employ security controls at alternate work sites:
  - Limit access to the area during CJI processing times to only those personnel authorized by Glencoe Police Department to access or view CJI.
  - Lock the area, room, or storage container when unattended.
  - Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
- Assess the effectiveness of controls at alternate work sites.
- Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Encryption
Reference: FBI CJIS Security Policy 5.10.1.2(5)

Glencoe Police Department City's IT Support uses public key infrastructure (PKI) technology only for technical management of desktop computers and servers through its Microsoft Systems Center Configuration Manager (MSCCM) administrative tool.

- Certificate shall be issued under the authority of a supervisor or a responsible official with the power to do so.
- A secure process that verifies the identity of the certificate holder shall accomplish issuance of a certificate.
- Issuing individual shall ensure that the certificate is issued to the intended party.
- All individual(s) involved in CA/RA shall be authorized access to CJI prior to accessing any information systems.
- The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in Administrator, CA Operations Staff, RAs, and Security Auditor trusted roles, and shall make them available during compliance audits. The RA shall maintain lists, including names, organizations, and contact information of those who act in RA Operations Staff, RA Administrators, and RA Security Auditor roles for that RA.
- Individual shall only have one role on the CA system.
- Physical access to CA equipment shall be limited to CA Operations staff and Security Auditors.
- All CA and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CA and RA equipment is prohibited. CA equipment shall be dedicated to performing CA functions. RA equipment shall be operated to ensure that the equipment meets all physical controls at all times

- Certificate shall be only valid for two years.
- New Certificate or re-keying requests shall be made by utilizing the formal process in place for initial request.
- Old or compromised certificate shall be immediately revoked.
- Certificate names and fields shall be unique, full and meaningful to minimize the possibility of vagueness of the ownership of the certificate(s).
- Certificate Revocation and Suspension
- CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder. Relying party client software may support on-line status checking and some support only CRLs. CAs should strongly consider offering online status checking in addition to CRLs.
- CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.
- Revocation requests shall be authenticated.
- Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.
- Circumstances for Revocation
- A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid.
- Examples of circumstances that invalidate the binding are:
    - Identifying information or affiliation components of any names in the certificate becomes invalid.
    - Privilege attributes asserted in the subscriber's certificate are reduced.
    - The subscriber can be shown to have violated the stipulations of its subscriber agreement.
    - There is reason to believe the private key has been compromised.
    - The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.
    - Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.
- Procedure for Revocation Request
    - A certificate revocation request shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a certification revocation are

detailed in the CPS.

- CRL Issuance Frequency
- CRLs shall be published within four (4) hours of generation. CRLs shall be issued periodically per the CPS, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.
- Certificate status information shall be published no later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.
- CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every eighteen (18) hours, and the next Update time in the CRL may be no later than forty-eight (48) hours after issuance time (i.e., the this Update time).
- CA private keys shall never be escrowed.
- A system backup shall be made when a CA system is activated. If the CA system is operational for more than a week, backups shall be made at least once per week. Backups shall be stored offsite. Only the latest backup needs to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system (shall meet all CJI/BCA requirements) unless the entire backup is containerized and encrypted to NIST Certified FIPS 140-2 Encryption.

Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actions correctly or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained. The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion.

- The validation, authentication, and handling of information in Certificate Applications.
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests,
- Renewal requests, or enrollment information.
- Issuance or revocation of Certificates, including personnel having access to restricted portions of its repository.
- Access to safe combinations and/or keys to security containers that contain materials supporting production services.
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINS that protect access to the HSMs.
- Providing enterprise customer support.
- Access to any source code for the digital certificate applications or systems.
- Access to restricted portions of the certificate repository.
- The ability to grant physical and/or logical access to the CA equipment.
- The ability to administer the background investigation policy processes.

Auditor

Security Auditors are responsible for auditing CAs and RAs. This sensitive role cannot be combined with any other sensitive role, e.g. the Security Auditor cannot also be part of the CA Operations Staff. Security Auditors are responsible for reviewing, maintaining, and archiving audit logs, and for performing or overseeing internal audits (independent of formal compliance audits) to ensure that CAs and RAs are operating in accordance with the associated CPSs.

Administrator

The administrator role shall be responsible for:

- Installation, configuration, and maintenance of the CA and CSS (where applicable)
- Establishing and maintaining CA and CSS system accounts
- Configuring certificate profiles or templates
- Configuring CA, RA, and CSS audit parameters
- Configuring CSS response profiles
- Generating and backing up CA and CSS keys
- Controlling and managing CA cryptographic modules
- System backups and recovery
- Changing recording media Administrators shall not issue certificates to subscribers

CA Operations Staff

The CA Operation Staff role shall be responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates
- Verifying the identity of subscribers and accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving and executing the revocation of certificates
- Approving infrastructure certificates issued to support the operations of the CA
- Approving revocation of certificates issued to CAs or to support the operations of the CA
- Approving certificates issued to RAs
- Authorizing RAs
- Approving revocation of certificates issued to RAs
- Providing Certificate revocation and suspension status information as part of a CSS (if 13 implemented)
- Posting Certificates and CRLs

RA Staff

RA Staff are the individuals holding trusted roles that operate and manage RA components. RA Staff is responsible for the following:

- Installation, configuration, and maintenance of the RA
- Establishing and maintaining RA operating system and application accounts
- Routine operation of the RA equipment such as system backup and recovery or changing

recording media
- Registering new Subscriber and requesting the issuance of certificates
- Verifying the identity of Subscribers
- Verifying the accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving, and executing the suspension, restoration, and revocation of certificates

Training Requirements

All personnel performing duties with respect to the operation of the CA, CSS or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/CSS/RA security principles and mechanisms
- All PKI software versions in use on the CA/CSS/RA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this policy

Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons shall present proof of the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role shall meet the following:

- Be employees of or contractor/vendor of the CA and bound by terms of employment or contract.
- Be appointed in writing.
- Have successfully completed an appropriate training program.
- Have demonstrated the ability to perform their duties.
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 1. Trusted Roles.
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties.

Voice Over Internet Protocol

Reference: FBI CJIS Security Policy 5.10.1.4(1)

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems.

- The Agency uses a hosted VoIP system that is managed by the City's IT Support.

- All network traffic from the VoIP system shall be segregated from data/CJDN traffic, through use of VLAN technology. (Appendix G.2 FBI CJIS SP outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.)
- The Agency shall establish usage restrictions and implementation guidance for VoIP technologies.
- The City's IT Support shall maintain overarching City VoIP phone system oversight, technical support and administration responsibilities.
- The Agency phone Administrator shall manage provisioning of voice mail services, resetting of voice mail passwords, phone activation and features on all phones utilized by the Agency.
- The City's IT Support phone system Administrator may perform on behalf of Agency, administrative actions pertaining to agency phones, when requested/directed by an Authorized Party of Agency.
- The phone System Administrator shall implement or oversee change of the default administrative password on the IP phones and VoIP switches.
- Passwords used for the administration and user operation of telephony system shall meet established complexity requirements:
    - Password cannot use extension number.
    - Password cannot use repeating digits.
    - Password must be a minimum of five digits passcode.

Patch Management
Reference: FBI CJIS Security Policy 5.10.4.1

The Glencoe Police Department IT Support shall be responsible for patch management of City information systems. The department shall:

- Centrally manage and routinely identify information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
- Identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
- Complete prompt installation and ensure software developer/vendor installation of newly released security relevant patches, updates, service packs and hot fixes, as well as fix patch requirements discovered during security assessments, vulnerability assessments, continuous monitoring or incident response activities.
- Have system administrator(s) patch their respective system(s) in a test environment(s) or groups prior to general deployment.

  Have LASO or designated personnel verify that patches are being applied in a timely fashion.
- Roll back patches that prove to have flaws or be incompatible.
- Automatically deploy and apply patches without user intervention.

- Have a formal risk acceptance process in writing, when vulnerabilities are found which will affect business operations.
- System administrator or LASO shall initiate a risk acceptance meeting with management along with stakeholders when patch(s) cannot be applied or failed due to unacceptable impact on systems and/or impact business operations; and management shall accept or direct System Administrator(s) for possible compensating controls to mitigate a vulnerability.

Security Alerts and Advisories
Reference: FBI CJIS Security Policy 5.10.4.4(3)

The Glencoe Department IT Support shall:
- Centrally manage security for all information systems.
- Conduct vulnerability and risk management operations to determine if any action needs to occur and notify appropriate LASO when corrective action is necessary.

LASO shall:
  - Sign up for and receive on a periodic basis security alerts and advisories that cover all appropriate software, hardware and firmware vulnerabilities and updates affecting the integrity of information systems or any data in information systems.
  - Configure systems, where possible, to automatically notify City's IT Support of any alerts. Alerts shall come from US CERT (https://www.us-cert.gov/ncas/alerts/index) or a reputable vendor.
  - Issue alerts/advisories to appropriate personnel for situational awareness
  - Document the types of actions to be taken in response to security alerts/advisories.
  - Take appropriate actions in response and notify the BCA via email at bca.iso@state.mn.us of any security incident(s) and conclusions.
  - Notify all relevant individuals in the Agency to initiate patch management, if required.

Mobile Devices
Reference: FBI CJIS Security Policy 5.13 and 5.13.1.1(13)

This policy area describes considerations and requirements for mobile devices including smart-phones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section supplement those in other areas of this Policy to address gaps introduced by using mobile devices.
- All information systems accessing CJI shall be maintained and managed by The City's IT Support on behalf of the Agency.
- Glencoe Police Department does not permit or allow personally owned devices and network equipment (BYOD).
- Any exception shall be documented and authorized in advance.

- City's IT Support shall verify that any user has a written and approved consent form, signed by head of Agency prior to allowing any personally owned system access to CJE.
- Mobile devices such as smart phones or tablets running an operating system that has not been approved by The City's IT Support shall be denied access to CJI.
- City's IT Support shall verify that unauthorized devices are removed from the CJE and LASO is notified of the violation.
- Mobile devices shall be enrolled in mobile device management (MDM) and provide compensating controls to meet all CJIS Security Policy and BCA Security Polices.
- Testing of access to devices while mobilized is done and remote wiping of devices is tested on a regular basis.
- City's IT Support personnel who enroll mobile devices into MDM shall test and document that all controls are functioning as intended for each device.
- Advanced authentication shall be utilized when accessing CJI from a mobile device from an unsecured location or using wireless connection.
- Any access to CJI must be done from within a secure physical location using a wired Ethernet connection or a wireless connection using City Virtual Private Network (VPN) client software, utilizing multi-factor authentication methods.
- Use of VPN shall be used when accessing information from mobile devices (I.e. squad laptops).
- NIST FIPS-140-2 encryption shall be utilized when accessing CJI Network over wireless or unsecured connection.
- City's IT Support personnel shall review the system logs for abnormalities.
- All individuals with mobile devices shall report loss or theft to the LASO.
- LASO shall report any loss or theft to the BCA at bca.iso@state.mn.us with a security incident form.

Wireless Access Restrictions
Reference: FBI CJIS Security Policy 5.13.1

This section applies to 802.11 WLAN, cellular, Wi-Fi, MiFi or Bluetooth or similar wireless technologies.

- Wireless network (WEP and WPAx) shall not be used to directly access criminal justice network environments. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.
- Authorized users shall connect through remote access VPN (compliant with required encryption standards) to gain access to CJI systems over wireless network, when such access required.
- NIST Certified FIPS 140-2 encryption tunnel shall be used to access CJE via wireless network.

- Advanced authentication shall be utilized when accessing CJE via wireless network outside of a secure facility or police conveyance.
- Wireless network shall be segmented (isolated) from CJE.
- Logs shall be maintained and reviewed at least monthly.
- Network appliances shall be disposed of in accordance with "Digital Media Sanitization and Disposal" section of this Policy.

The following controls shall be implemented for all City-managed wireless access points having access to any internal network that processes unencrypted CJI:

- Validation testing shall be performed to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
- A complete inventory of all Access Points (APs) and 802.11 wireless devices shall be maintained.
- Wireless Access Point equipment shall be placed only in secured areas, to prevent unauthorized physical access and user manipulation.
- Range boundaries shall be tested on Wireless Access Point equipment to determine the precise extent of the wireless coverage and design/tune the system to provide coverage only to areas needed for operational purposes.
- User authentication and encryption mechanisms shall be enabled for the management interface of Wireless Access Point equipment.
- All Wireless Access Point equipment shall use strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1 FBI CJIS Security Policy.
- Reset function on Wireless Access Point equipment shall be used only when needed and only invoked by authorized personnel.
- Wireless Access Point equipment shall be restored to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
    - Default service set identifier (SSID) in the access points shall be changed.
    - Broadcast SSID feature shall be disabled so that the client SSID must match that of Wireless Access Point equipment.
    - SSID character string shall be validated such that it does not contain any Agency identifiable information (division, department, street, etc.) or services.
- Security features of the wireless product shall be enabled, including the cryptographic authentication, firewall, and other available privacy features.
- Encryption key sizes shall be set to at least 128-bits and unique keys shall replace the default shared keys.
- Ad hoc mode shall be disabled.

- Non-essential management protocols on the Aps shall be disabled.
- All management access and authentication shall occur via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Non-FIPS compliant secure access shall be disabled to the management interface.
- Logging shall be enabled (if supported) and the logs reviewed on a recurring basis, at a minimum interval of monthly.
- Isolate the wireless network from the operational wired infrastructure through virtual local area network (VLAN) and ACLs or physically using firewalls. Access shall be limited between wireless networks and the wired network sufficient to meet only required operational needs.
- Access point configurations shall be cleared, when disposing of access points that will no longer be used, to prevent disclosure of network configuration, keys, passwords, etc.

Bluetooth
Reference: FBI CJIS Security Policy 5.13.1.3

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. This policy section shall dictate the use of Bluetooth and its associated devices based on the Agency's operational and business processes.

- Agency shall use NIST Certified FIPS 140-2 encryption tunnel in conjunction with advanced authentication to access CJE via Bluetooth network.
- Bluetooth devices shall not be used unless it has been approved by the BCA.
- Bluetooth shall be disabled on all devices, removed if possible.

Incident Response
Reference: FBI CJIS Security Policy 5.13.5

Security Incident-related information shall be obtained from a variety of sources including, but not limited to direct notification by end users, audit monitoring, network/systems monitoring, physical access monitoring, and user/administrator reports.

- Information security events and weaknesses shall be communicated in a manner allowing timely corrective action to be taken.
- In the event of an accidental or malicious information system security incident, the Agency and City's IT Support shall work together to properly mitigate the risk of CJI access.

- Lost, stolen or compromised devices shall be immediately reported to the Department of Information Systems.
- City's IT Support shall immediately implement and document appropriate steps to mitigate the risk of unauthorized access to CJI.
- Upon suspicion of a compromised system, Department of Information Systems, the Agency, or the individual shall immediately disconnect the system from the rest of the network.
    - Devices that are controlled through the MDM solution shall be locked and located if possible using system tools and local law enforcement assistance.
    - If location is not possible, devices are to be remotely wiped through the MDM solution.
    - LASO shall notify BCA of the lost equipment and submit an incident response form F.1 from CJIS Security Policy.
- City's IT Support and the Agency shall document:
    - Suspected cause for incident (Name of the malware, virus, etc.)
    - Whether security software was running at the time of infection.
    - How and when the problem was first identified.
    - When City's IT Support was notified.
    - Number of devices/systems affected.
    - Other connected equipment affected.
    - Action plan for removal.
    - CJIS data or personnel identification information compromised.
    - Equipment lost, stolen or compromised:
    - Was the device known to be locked?
    - Was the device outside of the United States?
- Once recovered and/or free from infection, the mobile device/system shall be reconnected.

Compliance and Personnel Sanctions
Reference: FBI CJIS Security Policy 5.12.4

In accordance with Section 5.12.4 of the FBI CJIS Security Policy a formal sanctions process shall be employed for personnel failing to comply with established information security policies and procedures.

Any employee misusing information or obtaining information for other than official criminal justice purposes from the Criminal Justice Data Network will be subject to disciplinary action.

1. Sanctions shall be administered after a review and evaluation of the totality of the circumstances including the severity of the inappropriate use.

2. If one or more individual users at an Agency are found to have inappropriate access to or use of one or more repositories or the secure network, the Agency shall take the following steps, including the following sanctions.

   a. Unauthorized access to the secure network by a user or department shall be terminated when possible.

   b. Inappropriate access to a repository shall place the Agency in non-compliant status and the Training and Auditing Unit shall work with the Agency to achieve compliance. Tools used include follow-up audits, tutoring, coaching, mentoring, and training.

   c. The first violation by an individual user shall result in training or the user's access will be suspended for a period not to exceed five (5) working days or both.

   d. A second violation by an individual user shall result in suspension of access for a period not to exceed thirty (30) calendar days and any other sanctions appropriate for the circumstances including, but not limited to, additional training or supervised system access.

   e. A third violation by an individual user may result in one or more of the following: suspension of access for longer than thirty (30) days, loss of access to other systems or tools that the individual uses, termination of access, or referral for criminal prosecution.

   f. Notwithstanding items 2.c through 2.e above, the totality of the circumstances may be so egregious that stronger sanctions are warranted and shall be imposed on a case-by-case basis.

ACCOUNTABILITY:

All members of the Department are responsible for ensuring that this and all other policies of the Department are followed. Deviations from this policy are permitted within the scope of authority granted all members of the Department; however, the deviation must be reported in accordance with policy 1.04 (Policy Deviations – Reporting Requirements).

Council Approved 6-7-21 TJP

Policy Updated 9-17-24 TJP

GLENCOE

SMALL CITY BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

GLENCOE
SMALL CITY BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

To: Mayor and City Council

From: Mark Larson, City Administrator

Date: October 7, 2024

RE: **Item 7C – Resolution 2024-12** Appointing the Election Judges for General Election

Item 7C – It is recommended to approve Resolution 2024-12 appointing the Election Judges for the 2024 General Election

RESOLUTION 2024-12

RESOLUTION DESIGNATING CITY OF GLENCOE ELECTION JUDGES
FOR THE GENERAL ELECTION TO BE HELD ON NOVEMBER 5th, 2024

WHEREAS, the election laws of the State of Minnesota provide that the governing body of a municipality must designate election judges for the municipality for the Primary Election:

NOW THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF GLENCOE, MINNESOTA.

That the following persons are hereby declared to be judges of the General Election to be held on Tuesday, November 5th, 2024 in the City of Glencoe.

Bonnie Hahn	Greg Ettel	Sarah Hueser
Cheryl Schmidt	Jodi Sell	Sharel Hoops
Connie Heitz	John McBride	Shari O'Donnell
Corey Schwanke	John Thell	Sharon Hoese
Deb Bargmann	John Winter	Steve Brelje
Deb Donnay	Kevin Dietz	Sue Terlinden
Dennis Oltmann	Lesa Hueser	Theresa Adrian
Eileen Harff	Michelle Miller	
Gary Schreifels	Paula Bulau	
Gary Ziemer	Renae Peterson	

Adopted and approved this 7th day of October, 2024.

_____
Ryan Voss, Mayor

ATTEST:

_____
Mark Larson, City Administrator

GLENCOE
SMALL CITY BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

GLENCOE

SMALL CITY BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

To: Mayor and City Council

From: Mark Larson, City Administrator

Date: October 7, 2024

RE: **Item 7D** – Prosecuting Attorney Fees

Item 7D – Attached is a request from Ken Jannsen to increase the fee for prosecuting Attorney fees from $145.00 per hour to $165.00 per hours.

It is the recommendation of the City Administration to **table** this request until staff can provide take a look at the number of billable hours over the past 5 years. I have attached a copy of the letter from Attorney Janssen in 2021 where the fee increased to $145 per hour with a cap of $60,000 in 2023 and 2024.

City of Glencoe
Office of the City Attorney

Kenneth G. Janssen
1017 Hennepin Avenue N. Glencoe, Minnesota 55336 Phone (320) 864-5142 Fax (320) 864-5146

September 18, 2024

Mark Larson
Glencoe City Administrator
1107 11th Street East, Suite 107
Glencoe, MN 55336

RE: City Prosecuting Attorney Services Hourly Rate

Dear Mark Larson:

A review of our records indicates that our current hourly rate is $145.00 for criminal (prosecutions) matters. This rate has been effective since January 1, 2022. We are now requesting to adjust the fee schedule to meet the changing needs of the City and our firm. If the new rate meets with your approval, as of January 1, 2025, the new rate will be $165.00 per hour. As always, your input is welcome. Please contact me if you wish to discuss the contents of this letter.

Sincerely,

Ken Janssen

Kenneth G. Janssen

City of Glencoe
Office of the City Attorney

Kenneth G. Janssen
1017 Hennepin Avenue N.$ Glencoe, Minnesota 55336 $ Phone (320) 864-5142 $ Fax (320) 864-5146

October 13, 2021

Mark Larson
Glencoe City Administrator
1107 11th Street East, Suite 107
Glencoe, MN 55336

RE: City Prosecuting Attorney Services Hourly Rate

Dear Mark Larson:

A review of our records indicates that our current hourly rate had been lowered from $145.00 to $125.00 for criminal (prosecutions) matters in 2019. In 2019, the firm had additionally agreed to cap all criminal prosecution fees at $50,000.00 per year for 3 years. We are now requesting to adjust the fee schedule to meet the changing needs of the City and our firm.

A review of the last three years shows that the firm has logged billable hours in the following amounts:

2019 : 425.35 hours x $125.00 = $53,168.75 (Capped at $50,000.00)
2020 : 445.15 hours x $125.00 = $55,643.75 (Capped at $50,000.00)
2021 : 391.15 hours (through September 30, 2021) x $125.00 = $48,893.75

As you can see, the 2019 adjustment has saved the City a considerable amount of money (over $25,000.00 plus the remainder of this year to be provided nearly free of any further attorney fees). The firm is now requesting to modify the fee schedule to $145.00 per hour, with a yearly cap of $55,000.00 in 2022 and then $60,000 in 2023 and 2024. If the new rate meets with the City's approval the new rate will commence on January 1, 2022. Please let me know if this increase is acceptable to the City of Glencoe. As always, your input is welcome. Please contact me if you wish to discuss the contents of this letter.

Sincerely,

Kenneth G. Janssen

GLENCOE

SMALL CITY BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

CITY OF GLENCOE BILLS

OCTOBER 7 , 2024

** PREPAID PAYROLL & WIRE TRANSFER BILLS **

VENDOR	DEPARTMENT: DESCRIPTION	TOTAL
CITY OF GLENCOE EMPLOYEES	MULTIPLE DEPTS.: CITY OF GLENCOE PAYROLL 7-10-24	$95,672.43
WIRE TRANSFER	MULT DEPTS: STATE SALES TAX	$27,773.00
WIRE TRANSFER	MULT DEPTS:EMP/CITY PAYROLL TAXES,HSA,PERA,D COMP,CAFE	$60,454.51
	TOTAL PREPAID BILLS ------>	$183,899.94

INVOICE APPROVAL LIST REPORT - SUMMARY BY VENDOR

OCT 7, 2024 - PREPAID BILLS

Date: 10/04/2024
Time: 11:30 am
Page: 1

City of Glencoe

Vendor Name	Vendor No.	Invoice Description	Check No.	Check Date	Check Amount
BREAKTHRU BEVERAGE	0513	LIQUOR: MERCH FOR RESALE	181926	07/10/2024	1,715.45
BREAKTHRU BEVERAGE	0513	LIQUOR STORE: MERCH FOR RESALE	181932	07/15/2024	2,000.84
				Vendor Total:	3,716.29
GLENCOE SPORTSMEN'S CLUB, IN	0836	ADMIN: FENCE IMPROVEMENTS	181933	07/15/2024	10,000.00
				Vendor Total:	10,000.00
JOHNSON BROS - ST PAUL	0504	LIQUOR: MERCH FOR RESALE	181927	07/10/2024	2,401.40
JOHNSON BROS - ST PAUL	0504	LIQUOR STORE: MERCH FOR RESALE	181934	07/15/2024	1,271.80
				Vendor Total:	3,673.20
MINNESOTA PUBLIC EMPLOYEE	1439	POLICE: UNION DUES	181935	07/15/2024	155.05
				Vendor Total:	155.05
PHILLIPS WINE & SPIRITS, INC.	1010	LIQUOR: MERCH FOR RESALE	181928	07/10/2024	1,182.35
PHILLIPS WINE & SPIRITS, INC.	1010	LIQUOR STORE: MERCH FOR RESALE	181936	07/15/2024	3,726.00
				Vendor Total:	4,908.35
SOUTHERN GLAZER'S OF MN	1429	LIQUOR: MERCH FOR RESALE	181929	07/10/2024	6,951.88
SOUTHERN GLAZER'S OF MN	1429	LIQUOR STORE: MERCH FOR RESALE	181937	07/15/2024	5,336.64
				Vendor Total:	12,288.52
VINOCOPIA, INC.	1353	LIQUOR: MERCH FOR RESALE	181930	07/10/2024	146.50
				Vendor Total:	146.50
WINE MERCHANTS	0667	LIQUOR: MERCH FOR RESALE	181931	07/10/2024	1,040.00
				Vendor Total:	1,040.00
				Grand Total:	35,927.91
				Less Credit Memos:	0.00
Total Invoices:	12			Net Total:	35,927.91
				Less Hand Check Total:	0.00
				Outstanding Invoice Total :	35,927.91

INVOICE APPROVAL LIST REPORT - SUMMARY BY VENDOR

OCT 7, 2024 - REGULAR BILLS

Date: 10/04/2024
Time: 10:52 am
Page: 1

City of Glencoe

Vendor Name	Vendor No.	Invoice Description	Check No.	Check Date	Check Amount
A.H. HERMEL CO.	0573	COUNCIL, PARK, REIMB,CITY CTR: MERCH FOR RESALE, SUPPLIES	0	00/00/0000	704.37
				Vendor Total:	704.37
AQUA PRO	1475	ADMIN: SPRINKLER SYSTEM WINTERIZATION	0	00/00/0000	351.00
				Vendor Total:	351.00
AXON ENTERPRISE, INC	0439	POLICE: CAMERA MOUNT	0	00/00/0000	31.30
				Vendor Total:	31.30
BME LAB AND SCIENCE	2290	WWTP: ANNUAL EQUIPMENT CALIBRATION	0	00/00/0000	367.99
				Vendor Total:	367.99
BRADLEY SECURITY & ELECTRIC	0209	MULT DEPTS: CAMERA SYSTEMS, REKEY	0	00/00/0000	6,805.50
				Vendor Total:	6,805.50
CARLSON, MORGAN & MATT	1325	CITY CENTER: DAMAGE DEPOSIT	0	00/00/0000	200.00
				Vendor Total:	200.00
CENTURYLINK	1394	MULT DEPTS: PHONE BILL	0	00/00/0000	842.89
				Vendor Total:	842.89
CHERRYROAD MEDIA, INC	0877	AQUATIC: ADVERTISING	0	00/00/0000	155.00
				Vendor Total:	155.00
COMPANION LIFE INSURANCE	1859	MULT DEPTS: INS PREMIUMS	0	00/00/0000	3,034.05
				Vendor Total:	3,034.05
CREATIVE PRODUCT SOURCING,	0732	POLICE: CERTIFICATES, PENCILS, STICKERS	0	00/00/0000	375.59
				Vendor Total:	375.59
DAKOTA SUPPLY GROUP	0523	WATER, WWTP: GATE VALVE, COUPLINGS, GASKETS, WIRE	0	00/00/0000	16,093.87
				Vendor Total:	16,093.87
EGGERSGLUESS, BRAD	0869	ADMIN: MONTHLY CELL PHONE REIMB	0	00/00/0000	50.00
				Vendor Total:	50.00
FLEET SERVICES DIVISION	2144	POLICE: SQUAD CAR LEASES	0	00/00/0000	4,217.17
				Vendor Total:	4,217.17
FRANKLIN PRINTING INC.	0085	WWTP: OFFICE SUPPLIES	0	00/00/0000	23.96
				Vendor Total:	23.96
FREITAG, BENTON	0659	CABLE TV: COUNCIL MEETING RECORDING	0	00/00/0000	100.00
				Vendor Total:	100.00
GACC TOURISM	0168	REIMB: LODGING TAX	0	00/00/0000	70.29
				Vendor Total:	70.29
GALLS, LLC	0452	POLICE: TRAINING SUPPLIES	0	00/00/0000	95.82
				Vendor Total:	95.82
GILLETTE PEPSI COMPANIES, INC	0496	LIQUOR: MERCH FOR RESALE	0	00/00/0000	461.00
				Vendor Total:	461.00
GLENCOE FIRE RELIEF ASS'N.	0455	FIRE: FIRE STATE AID & SUPPLEMENTAL BENEFIT	0	00/00/0000	64,675.39
				Vendor Total:	64,675.39
GOPHER STATE ONE CALL	0482	WATER, WWTP, STORM WATER: LOCATE TICKETS	0	00/00/0000	114.75
				Vendor Total:	114.75
HALQUIST, AMY	1946	FINANCE: UNIFORMS	0	00/00/0000	200.00
				Vendor Total:	200.00
HAWKINS, INC.	1133	AQUATIC, WATER, WWTP: CHEMICALS	0	00/00/0000	10,282.79
				Vendor Total:	10,282.79

Vendor Name	Vendor No.	Invoice Description	Check No.	Check Date	Check Amount
HERALD JOURNAL PUBLISHING	1442	ADMIN, SANITATION: PUBLISHING, ADVERTISING	0	00/00/0000	342.98
				Vendor Total:	342.98
HILLYARD HUTCHINSON	0122	ADMIN: CLEANING PRODUCTS	0	00/00/0000	1,397.99
				Vendor Total:	1,397.99
HYDRO ENGINEERING, INC.	0554	WWTP: CAMLOCK	0	00/00/0000	25.22
				Vendor Total:	25.22
INDEPENDENT SCHOOL DIST. #28	0128	REIMB: WASTE MANAGMENT REFUND	0	00/00/0000	207.73
				Vendor Total:	207.73
INTERSTATE ALL BATTERY CENTE	2111	WATER, WWTP: BATTERIES	0	00/00/0000	43.20
				Vendor Total:	43.20
JOHNSON CONTROLS FIRE	0874	ADMIN, POLICE: FIRE EXTINGUISHERS, SENSOR	0	00/00/0000	752.25
				Vendor Total:	752.25
KDUZ - KARP - KGLB	2248	ADMIN, LIQUOR: ADVERTISING	0	00/00/0000	1,552.00
				Vendor Total:	1,552.00
KLOCKMANN, MITCHEL & ISABELL	1670	CITY CENTER: DAMAGE DEPOSIT REFUND	0	00/00/0000	200.00
				Vendor Total:	200.00
KUSLER, HAYLIE	2138	ADMIN: MILEAGE REIMB.	0	00/00/0000	92.46
				Vendor Total:	92.46
KWIK TRIP	1653	POLICE: FUEL	0	00/00/0000	2,075.78
				Vendor Total:	2,075.78
LEAGUE OF MINNESOTA CITIES	0154	ADMIN: MEMBERSHIP DUES	0	00/00/0000	2,390.00
				Vendor Total:	2,390.00
LITZAU EXCAVATING	0380	WWTP: MANHOLE RINGS, SLIP LINE SEWER	0	00/00/0000	1,370.44
				Vendor Total:	1,370.44
LONDERVILLE, ANNIKA & GRAYSC	2020	CITY CENTER: DAMAGE DEPOSIT REFUND	0	00/00/0000	100.00
				Vendor Total:	100.00
MCLEOD COOP. POWER ASS'N.	0201	ADMIN, AIRPORT: ELECTRICITY	0	00/00/0000	696.13
				Vendor Total:	696.13
METRO SALES, INC	1066	ADMIN, POLICE: OFFICE EQUIPMENT LEASE	0	00/00/0000	593.27
				Vendor Total:	593.27
MINI BIFF	0177	PARK, SANITATION: WASTE REMOVAL	0	00/00/0000	790.50
				Vendor Total:	790.50
MN DEPT. OF HEALTH	1223	WATER: SUPPLY SERVICE CONNECTION FEE	0	00/00/0000	4,911.00
				Vendor Total:	4,911.00
MN FIRE SERVICE CERT. BOARD	0557	FIRE: FIREFIGHTER RECERTIFICATIONS	0	00/00/0000	210.00
				Vendor Total:	210.00
MVTL , INC.	0353	WWTP: LAB TESTING	0	00/00/0000	1,926.00
				Vendor Total:	1,926.00
NORTH CENTRAL LABORATORIES	0631	WWTP: LAB SUPPLIES	0	00/00/0000	2,808.25
				Vendor Total:	2,808.25
NUVERA	2120	MULT DEPTS: INTERNET, PHONE, IT SUPPORT	0	00/00/0000	5,052.06
				Vendor Total:	5,052.06
OEM SERVICE CO, LLC	0937	WWTP: TRUCK REPAIR	0	00/00/0000	119.21
				Vendor Total:	119.21
PLUNKETT'S PEST CONTROL, INC	0446	ADMIN: PEST CONTROL	0	00/00/0000	236.94
				Vendor Total:	236.94

Vendor Name	Vendor No.	Invoice Description	Check No.	Check Date	Check Amount
PRO AUTO GLENCOE, INC	0527	STREET, WATER: TIRE, OIL CHANGE	0	00/00/0000	378.31
				Vendor Total:	378.31
RELIANCE STANDARD LIFE INS CC	1915	MULT DEPTS: INS PREMIUMS	0	00/00/0000	895.82
				Vendor Total:	895.82
SCHMITT, STEVE	1696	WATER: HOTEL, TRAVEL EXPENSE REIMB	0	00/00/0000	440.20
				Vendor Total:	440.20
SEH	1757	ADMIN, MSA, '23 STREET IMPROV: ENGINEERING	0	00/00/0000	5,807.75
				Vendor Total:	5,807.75
STAR GROUP, L.L.C.	0972	STREET, PARKS, WWTP: OIL, FITTINGS, HOSES, FILTERS	0	00/00/0000	374.24
				Vendor Total:	374.24
STUEWE, MATT	0922	WATER: SAFETY SHOES	0	00/00/0000	139.99
				Vendor Total:	139.99
USA BLUEBOOK	1693	WATER: LAB SUPPLIES	0	00/00/0000	23.95
				Vendor Total:	23.95
VANDAMME, JON	0136	LIQUOR: MONTHLY CELL PHONE REIMB, UNIFORM	0	00/00/0000	250.00
				Vendor Total:	250.00
VANDAMME, MYRANDA	0028	CITY CENTER: MONTHLY CELL PHONE REIMB, UNIFORMS	0	00/00/0000	250.00
				Vendor Total:	250.00
VERIZON WIRELESS	1110	POLICE: SQUAD CAR PHONES	0	00/00/0000	200.05
				Vendor Total:	200.05
VOIGT, JAMES	1894	STREET: LIGHT SWITCH, VALVES	0	00/00/0000	145.15
				Vendor Total:	145.15
VOSS, RYAN	2217	ADMIN: MONTHLY CELL PHONE REIMB	0	00/00/0000	50.00
				Vendor Total:	50.00
WL HALL CO INTERIOR SERVICE	0858	CITY CENTER: ANNUAL WALL INSPECTION	0	00/00/0000	985.00
				Vendor Total:	985.00
WM. MUELLER & SONS, INC.	0206	STREET: SAND	0	00/00/0000	919.59
				Vendor Total:	919.59
ZERO9 HOLSTERS	2028	POLICE: UNIFORM ACCESSORIES	0	00/00/0000	194.75
				Vendor Total:	194.75
				Grand Total:	148,200.94
				Less Credit Memos:	0.00
Total Invoices:	60			Net Total:	148,200.94
				Less Hand Check Total:	0.00
				Outstanding Invoice Total :	148,200.94

GLENCOE
SMALL CITY & BIG FUTURE

City of Glencoe ♦ 1107 11th Street East, Suite 107 ♦ Glencoe, Minnesota 55336
Phone: (320) 864-5586 Website: www.glencoemn.org Email: info@ci.glencoe.mn.us

This page is blank to separate agenda items.

FUND BALANCES

FUND #	2024 CASH BALANCES	MONTH JUNE	MONTH MAY	MONTH APRIL
101	General-Operating	$ 1,900,071.01	$ 860,752.23	$ 1,389,383.18
101	General-Childhood Intervention	$ 886.55	$ 886.55	$ 886.55
101	General-Crime Prevention	$ 11,059.42	$ 11,059.42	$ 11,059.42
601	Water-Operating	$ 2,404,178.21	$ 2,306,457.27	$ 2,261,741.81
601	Water-Water Availability Charge	$ 594,275.03	$ 589,790.31	$ 588,885.35
601	Water-Trunk Water Charge	$ 25,748.16	$ 25,719.13	$ 25,690.56
601	Water-Bonds	$ 1,955.61	$ 1,953.41	$ 1,951.24
601	Water-Construction	$ -	$ -	$ -
602	W.W.T.P.-Operating	$ 1,676,074.32	$ 1,644,449.81	$ 1,647,271.16
602	W.W.T.P.-Sewer Availability Charge	$ 1,131,931.50	$ 1,127,915.95	$ 1,126,413.14
602	W.W.T.P.-Trunk Sewer Charge	$ 131,328.00	$ 131,179.96	$ 131,034.22
602	W.W.T.P.-Bonds	$ 357,224.97	$ 288,589.28	$ 220,034.56
602	W.W.T.P.-Construction	$ -	$ -	$ -
603	Sanitation	$ 44,012.88	$ 43,346.84	$ 44,629.23
604	City Center-Operating	$ (25,181.08)	$ (91,410.60)	$ (27,590.30)
604	City Center-Bonds	$ (682,982.84)	$ (682,212.93)	$ (681,455.01)
609	Liquor Store	$ 123,132.60	$ 78,624.59	$ 62,222.80
612	Airport	$ (238,341.85)	$ (172,442.77)	$ (139,691.45)
651	Storm Water Management	$ 113,955.71	$ 81,270.44	$ 57,705.57
213	Park Improvement	$ 176,456.73	$ 168,666.38	$ 164,683.22
223	Aquatic Center	$ (29,984.51)	$ (9,721.28)	$ (4,286.94)
223	Aquatic Center-Lifeguard Training	$ 997.90	$ 574.90	$ 2,295.25
225	Cable TV	$ 8,972.34	$ 9,062.11	$ 4,009.31
226	Cemetery	$ (14,297.01)	$ (12,057.04)	$ (2,272.14)
229	Municipal State Aid	$ 47,840.00	$ 47,962.87	$ 80,667.58
230	Engineering/Inspection Services	$ (112,773.54)	$ (112,646.41)	$ (112,521.26)
231	Public Safety Aid	$ 199,038.70	$ 220,403.00	$ 221,453.00
300	City Sinking	$ 410.31	$ 406.27	$ 405.82
382	2007 Tax Increment Bond-2007 Industrial Park	$ (58,365.28)	$ (58,299.49)	$ (58,234.72)
384	2018 Tax Increment Bond-Panther Heights	$ (32,526.74)	$ (32,490.07)	$ 72.35
409	Tax Increment #4-Industrial Park	$ 434,622.65	$ 434,132.71	$ 433,650.40
424	Tax Increment #17-Miller Manufacturing	$ 34,157.28	$ 23,874.81	$ 23,848.29
426	Tax Increment #19-Panther Heights	$ 73,071.83	$ 1,576.67	$ 1,574.92
427	Tax Increment #20-Bus Garage	$ (9,721.31)	$ (9,710.35)	$ (9,699.56)
466	2023 Street Improvement	$ (7,499.70)	$ (6,713.22)	$ (6,475.02)
523	2008 11th Street/Morningside Bond	$ 73,782.60	$ 11,549.87	$ 11,537.04
524	2014 Street Improvement Bond	$ (110,138.95)	$ (214,171.71)	$ (213,933.77)
525	2015 Street Improvement Bond-Lincoln Park	$ 56,440.84	$ (49,194.21)	$ (49,139.56)
526	2016 Street Improvement Bond-Armstrong Avenue	$ 143,876.28	$ 95,834.06	$ 95,727.59
527	2017 Street Improvement Bond-Baxter Avenue	$ 186,556.43	$ 87,521.91	$ 87,424.68
528	2018 Storm Water Improvement Bond-Central Storm Sewer	$ 166,340.31	$ 78,909.70	$ 78,822.03
529	2021 Street Improvement Bond-10th Street	$ 87,563.10	$ 64,746.76	$ 66,064.78
530	2023 Street Improvement Bond	$ 5,196.69	$ (35,287.45)	$ (35,248.25)
	TOTALS	$ 8,889,345.15	$ 6,950,859.68	$ 7,500,597.07

CITY OF GLENCOE
DEPARTMENT SUPERVISOR
MONTHLY SUMMARY Report
Department: Wastewater Treatment Plant (WWTP)

Supervisor Name: Ron VonBerge **Month/ August 2024**

Below is a review of tasks completed during the previous month...

Weekly check of Glen Knoll lift station (4 X) **I/I inspections**

Weekly plant maintenance task (4 X) DMR and QA/QC data entry

Lab testing and daily task.

Week of 8/5/24/2024

Replaced 2 UV bulbs.
Brought camera to get repaired.
Monthly generator testing
Hauling biosolids
Jetting collection system
Mowed lawn
Jetted and Hydro vaced storm line by Oak Leaf Park Road.

Week of 8/12/2024

Hauling biosolids
Jetting
Replaced 4-disc filter panels.
Decanting secondary digester
Weed Whip WWTP and impound lot.

Week of 8/19/2024

Hauling Biosolids
Jetting sewer lines.
Lowered manholes and water shut offs, so snowplows don't hit them
Decanting secondary digester.
Cleaned static mixer.

Week of 8/26/24

Bio solids hauling
Jetting
Decanting secondary digester
Cleaned blower inlet filters
Yearly cleaning of Grit Vortex chamber
Transferred secondary digester to biosolids tank
Weed whip WWTP
Mowed lawn WWTP

Glencoe Municipal Liquor Store
Profit & Loss Statement for June 2024

Sales	
Liquor	84,537.93
Beer	140,006.21
Wine	15,021.10
Other Merchandise	6,117.82
THC	1,072.47
Total Sales	246,755.53
Cost of Sales	
Beginning Inventory	480,191.80
Purchases	170,168.26
Total Merch. Avail. for Sale	650,360.06
Less Inventory Ending	467,310.04
Cost of Sales	183,050.02
Gross Profit on Sales	63,705.51
	25.82%
Operating Expenses	
Sales Tax (Use tax)	102.00
Full-Time Employees	6,402.00
Full-Time Employees- Overtime	0.00
Part-Time Employees	6,055.56
PERA Contributions	850.53
FICA Contributions	764.82
Medicare Contributions	178.84
Health & Life Insurance	2,204.00
Operating Supplies	5,082.51
Cleaning Supplies	0.00
Repair & Maintenance	907.78
Professional Services	0.00
Training	0.00
Computer Repair/Equipment	310.69
Telephone	116.89
Travel Expense	0.00
Advertising	812.00
Printing & Binding	0.00
Electricity	870.05
Natural Gas	86.74
Uniforms	632.00
Miscellaneous	0.52
Sub-total	25,376.93
Insurance- Liquor, Property, Gen'l Liability	766.04
Depreciation	3,504.41
Audit	250.00
Worker's Comp	308.62
Bond Interest	841.04
Total Operating Expenses	31,047.04
Non-Operating Expenses/Income	
Interest Income	88.73
Miscellaneous	1,100.01
Sales Tax Variance	2.23
Cash Drawer +/-	(14.95)
Bad/Collected Checks	0.00
Total Non-Operating Exp./Inc.	1,176.02
Net Income	33,834.49
Year-To-Date Income	140,646.93

Comparative Figures	
Previous Year (2023)	
Total Sales	268,985.64
Gross Profit on Sales	70,615.68
Total Operating Expenses	36,254.39
Total Non-Operating Exp./Inc.	(343.09)
Net Income	34,018.20
Year-To-Date Income	110,227.56

Current YTD Cash Balance	123,132.60
Last Month YTD Income	106,812.44