IDAHO STATE POLICE PROCEDURE

02.22 FACILITY ACCESS AND SECURITY

I. General

    A. The Idaho State Police (ISP) is firmly dedicated to safeguarding the well-being of its employees, visitors, and the protection of its facilities and infrastructure. Our commitment to safety extends to both electronic and physical security, and this policy sets forth the guidelines for controlling and verifying access to ISP facilities for all individuals seeking electronic and/or physical entry.

    B. Our primary goal is to create a secure environment where access is controlled, authorized, and monitored, ensuring the utmost safety and confidentiality for our personnel and sensitive assets. This policy serves as a framework to achieve these objectives and maintain the integrity of ISP facilities.

II. Definitions

    A. "Authorized Personnel" is any individual who has successfully undergone a comprehensive background investigation conducted by ISP or has received full approval from the designated ISP HQ Hiring Captain to meet ISP employee-level access requirements. Examples include ISP Employees, personnel from other law enforcement agencies with daily access needs (e.g., Fusion Center, Task Force members), Public Safety Communications (PSC) staff, and State Comm/Department of Health and Welfare (DHW) personnel.

    B. "Authorized Access Card" is an ISP-produced access card issued to "Authorized Personnel" for granting access.

    C. "Critical Areas" are areas or rooms containing, but not limited to, sensitive law enforcement information, criminal history information, personal identifying information, financial information, physical files, servers, routers, networked computers or other equipment, personnel files, evidence, laboratories, control centers, equipment storage areas, armories, radios, radio programming and installation equipment, communications centers, and terminals that access any of the above-listed data and are accessible only by "Authorized Personnel."

    D. "Electronic Access" means access through any electronic means to any ISP owned, controlled, or operated network, portal, server, system, or data from any location outside an ISP facility.

    E. "Escort" refers to the immediate physical presence and visual supervision of an individual to prevent access to protected information or areas.

    F. "ISP Facilities" include any building, room, or area owned, leased, or controlled by ISP personnel, with access restricted by physical barriers such as locked doors, gates, fences, or other means.

G. "Non-ISP personnel" refers to any individuals who are not considered ISP employees but are contracted or engaged in activities with the sole intention of providing services, products, or information to ISP. They must have passed a fingerprint-based background check, meet ISP access requirements, and receive approval from the designated ISP HQ Hiring Captain and Idaho CSC. Examples include retirees, contractors, cafeteria staff, POST actors and graders, vendors, volunteers, or others who would not be subjected to a full ISP background investigation.

H. "Limited Access Card" is an ISP-produced authorized access card, typically in the form of a proximity card, issued to a particular person to grant access to ISP facilities. This card is orange in color.

I. "Retired Access Card" is an ISP-produced authorized access card issued to ISP personnel who retire in good standing and request access to ISP facilities.

J. "Visitor" is a person who is temporarily (generally a week or less) visiting an ISP facility, who will be escorted in critical areas, and who may need to access non-critical areas such as, but not limited to, conference rooms, classrooms, restrooms, break rooms, and common hallways.

K. "Visitor ID Card" is an ISP-issued identification card provided to a particular person visiting an ISP facility. This card is for identification purposes and does not grant physical access to the facility. This card is green in color.

L. "Visitor Log" is a log maintained by each program which must contain the name, date(s) of access, access card number, company (if applicable) and reason for access.

III. ISP Facilities Access

A. All Authorized Personnel, non-ISP Personnel, and visitors, except ISP Troopers in uniform defined in ISP Procedure 02.03 Grooming and Dress Section (C)(1-16), must wear and prominently display an ISP issued access card while in an ISP Facility.

B. No personnel will be allowed entrance to an ISP facility without a properly issued card, except;
   1. personnel who are being escorted by an authorized person.
   2. personnel attending approved planned events such as graduations, rallies, public meetings, press conferences, etc. Access for these types of events shall be limited to non-critical areas.

C. Personnel displaying a Limited Access or Visitor Access card shall not escort anyone.

D. Visitors must be escorted by an authorized person in critical areas.

E. Personnel wearing a "Visitor ID Card" may have unescorted access to non-critical areas such as, but not limited to, conference rooms, classrooms, restrooms, break

rooms, and common hallways.

F. Any personnel who have been granted access to critical areas without a properly issued card, and the personnel who allowed such improper access, if applicable, will both be in violation of this procedure.

G. Any visitor or Limited Access personnel violating this procedure may be immediately escorted from the ISP Facility, and their access privileges may be revoked permanently.

IV. Access Cards

A. All access cards will be issued and valid for five years from the date of the individual's photograph, which will be displayed on the card, to ensure that the photograph and other depicted information are accurate and current.

B. All access cards will contain the following on the back side: "If found, return to Idaho State Police, 700 S. Stratford Drive, Meridian, ID, 83642, phone 208-884-7000."

V. ISP Access Cards

A. All new Authorized Access Card requests are initiated by ISP Human Resources using the ISP Security Form.

B. Access adjustments, modifications, or replacement of lost cards are requested by a supervisor to HR and initiated utilizing the ISP Security Form.

C. Temporary access cards may be issued to an employee that has misplaced or forgotten their access card.

D. To ensure accountability, a log shall be maintained to track the issuance and return of temporary access cards.

E. District Commanders are responsible for overseeing the proper issuance and return of temporary access cards within their respective districts.

VI. Card Appearance

A. The card depicts the employee photograph, employee name, ISP shoulder patch, program, the words "Idaho State Police", and the five-year photo expiration date.

B. ISP Access Cards must be printed and oriented in a portrait or vertical configuration.

VII. Renewals

1. The IT Network Operations Center will provide a monthly report to the IT Administrative Assistant of all Access Cards expiring the next month or upcoming expirations.

2. The IT Administrative Assistant will disperse the report to each Program Manager.

3. The District Captain or Program Manager notifies the employee that within 10 days, the employee will need to arrange with the district's responsible party for obtaining a new photograph according to Section "E."

4. HR will create a security form, attach the updated photo, and route it to IT.

5. ISP IT will update the photo and the Employee Directory, create, and deliver the new access card to HR for issuance.

VIII. Limited Access Cards

A. The ISP contact sends a link to the requestor with instructions on how to complete the ISP Access Request Form.

B. The requestor completes the form as per the provided instructions.

C. The ISP contact reviews the submitted form and specifies the correct access requirements.

D. The form is then forwarded to ISP HR for coordination of fingerprint cards and photos.

E. HR uploads the digital photo to the ISP Access Request Form.

F. HR routes the ISP Access Request Form directly to BCI and sends the hard copy of the fingerprint card to BCI within three days of receipt of a completed packet.

G. BCI will approve or deny access based on CJIS Security Policy guidelines and will attach the results of the fingerprint-based background check to the Secured Attachments Section of the ISP Access Request Form.

H. The form is routed to the ISP HQ Hiring Captain for approval or disapproval.

I. If approved:
   1. The ISP Access Request Form is then routed to ISP IT.
   2. Prior to issuing a disapproval, the ISP HQ Hiring Captain will consult with ISP HR to ensure that the denial is appropriate based on the access requested. If access is only requested to non-critical areas, or the person can be escorted, then access may be granted at the concurrence of the ISP HQ Hiring Captain and ISP HR.

J. If disapproved:
   1. HR completes the form and notifies the requestor.
   2. IT grants the requested access and prints the access cards where necessary. IT completes the form and delivers the printed access card to ISP HR.

K. ISP access requests will expire automatically based on the following:
   1. State of Idaho Employees' access will expire in five years.

IDAHO STATE POLICE PROCEDURE

2. Contractors' access will expire in two years.

IX. Card Appearance

A. The card depicts the person's photograph, name, company name or purpose (Motorola, etc.), the words "Idaho State Police", the words "Limited Access" and five-year card expiration date.

B. Cards must be printed and oriented in a landscape or horizontal configuration.

X. Renewals

A. The ISP point of contact listed on the ISP Access Request Form (section D (2) above) will receive a system generated notification that the Non-ISP Access will be expiring within the next 30 days.

B. If the relationship will continue, and the limited access has not expired, then the point of contact pulls up the completed ISP Access Request Form and updates the new expiration date, adds a comment that they wish to renew and forwards that to ISP HR.

C. ISP HR ensures a name-based background check is completed. The results of the name-based check are uploaded to the Secured Attachment section and sent to the ISP HQ Hiring Captain for approval or disapproval.

D. If approved, HR will then route the approved form to ISP IT who will update the expiration date. IT will mark the form as complete then forward the completed form to the original ISP requestor. No access card is printed.

E. Prior to issuing a disapproval the ISP HQ Hiring Captain will consult with ISP HR to ensure that the denial is appropriate based on the access requested. If access is only requested to non-critical areas, or the person can be escorted, then access may be granted at the concurrence of the ISP HQ Hiring Captain and ISP HR.

F. If disapproved, HR completes the form and notifies the requestor.

G. If the access has expired, the ISP Access Request Form must be processed as a new request, to include new fingerprint cards, photo, and proximity cards where needed.

H. If the card is due to or has expired, a new photograph must be taken and attached in accordance with the requirements listed in section E., below. No photo is needed for digital access only.

XI. Retired Access Cards

A. Issuance
    1. Requests for access are made utilizing the ISP EHF 03-04-06 Separation Form.
    2. Photographs must be taken and attached in accordance with the

requirements listed in section E., below.

    2. Card Appearance
        1. The card depicts the employee photograph, employee name, ISP shoulder patch, the words "Idaho State Police" and "Retired", and the five year card expiration date.
        2. Retired Access Cards must be printed and oriented in a portrait/vertical configuration.

XII.   Visitor ID Card

    A. Issuance.
        1. Programs issuing Visitor ID cards shall confirm the visitor's identity and log the visitor's name, reason for visit, time in and time out, and the access card number being checked out.
        2. The program will maintain the Visitor Log.
        3. Visitor ID Cards may be issued to a person needing access for limited durations, typically one week or less.
        4. All Visitor ID Cards must be returned to the issuing program.

    B. Card Appearance
        1. The card bears the word "Visitor", the program issuing the card, the ISP shoulder patch, the words "Idaho State Police", and a unique number which corresponds to a visitor log.
        2. Visitor cards must be printed and oriented in a landscape/horizontal configuration.

XIII.   Lost, Stolen, Destroyed, or Forgotten Authorized Access Cards

        1. Any person who, upon the discovery of or knows their ISP issued card has been lost, stolen, or destroyed, must promptly notify their immediate supervisor or ISP point of contact.

        2. Any person who forgets their card and needs access must be issued a "Temporary ISP Access Card".

        3. Lost, stolen, or destroyed cards are replaced in accordance with Section D – Access Cards.

XIV.   Card Photographs

    A.   Commissioned personnel must wear a Class A uniform including cover, Lieutenants and above will be in the ISP Dress Uniform.

    B.   Non - Commissioned personnel must wear business attire.

    C.   Retiring personnel must wear business attire, regardless of prior duties.
    D.   Limited Access personnel must wear attire commensurate with their duties and/or role.

E. Limited Access photographs may deviate from the below listed requirements where necessary when it is unreasonable to obtain an ISP taken photograph. In that instance the photograph should match as many of the elements as possible defined in Section 6., below.

F. Photographs are taken using the following guidelines and equipment:
1. The issued iPhone is utilized as the camera, utilizing the issued tripod mounted holder, tripod, light, and remote shutter.
2. The above listed equipment has been issued to each ISP District office, POST, and ISP HR. Photos will be taken by personnel at those locations.
3. Photos are taken in a portrait fashion, with the subjects' torso and head squarely facing the camera, utilizing the issued backdrop.
4. The backdrop is placed, then the front of the light/tripod assembly is placed approximately 42 inches (the length of the backdrop carrying case) from the backdrop.
5. On the iPhone, turn on the grid feature (settings/camera/grid) and then pair the remote shutter to the iPhone (settings/Bluetooth/select ABShutter).
The camera flash and "Live" photo features are turned off, and the HDR set to auto (icons located on the top banner of the camera screen).
6. The iPhone is positioned with the holder clasping the bottom portion of the iPhone. The height of the light/iPhone is set where the top of the iPhone is positioned at approximately the same level as the subject's nose.
7. The ring light color is set to 4500K, and the light intensity is set to 30%.
8. The subject stands as close to the backdrop as possible without touching the backdrop.
9. Adjust the zoom on the phone and/or the phone angle to ensure the outer edges of the shoulders fit just inside the display. The top horizontal gridline should be positioned at the subject's eye level. Ensure the remote shutter is utilized to take the photo.

XV. Photo Upload

A. After photos are taken, they must be uploaded to the ISP Portrait App, entering First and Last name and District/Department, choosing the photo file then submit.

B. The App uploads the photo directly to the Imported Raw Photos Folder to be attached to the Security Form.

C. A notification of upload is sent to HR.