OFFICE OF ADMINISTRATION,
DIVISION OF FACILITIES MANAGEMENT, DESIGN & CONSTRUCTION
AUTHORIZATION FOR RELEASE OF INFORMATION CONFIDENTIALITY OATH

Legal Name as it appears on Driver's License or State Issued ID	Vendor/Contracting Company Name
Social Security Number	Date of Birth

Building Address list each building on a separate line	Contract/Project Number	Badge Information Please indicate specific days and times below
EXAMPLE: 123 MAIN STREET, CITY, STATE, ZIP	123456	Is Proxy Badge Access Needed? ☑ Yes ☐ No **If yes:** Days of Week Mon - Fri Times 8a-5p
		Is Proxy Badge Access Needed? ☐ Yes ☐ No **If yes:** Days of Week Times
		Is Proxy Badge Access Needed? ☐ Yes ☐ No **If yes:** Days of Week Times
		Is Proxy Badge Access Needed? ☐ Yes ☐ No **If yes:** Days of Week Times
		Is Proxy Badge Access Needed? ☐ Yes ☐ No **If yes:** Days of Week Times
		Is Proxy Badge Access Needed? ☐ Yes ☐ No **If yes:** Days of Week Times

I hereby authorize and request release to the State of Missouri, Office of Administration, Division of Facilities Management, Design & Construction, any and all records and information, including, but not limited to, originals or copies of any records, documents, reports, and criminal history record.

I understand that the Office of Administration, Division of Facilities Management, Design & Construction, may conduct and/or review a background investigation before rendering a decision regarding my eligibility to perform services for the Office of Administration, Division of Facilities Management, Design & Construction, and that this authorization is a part of that investigation.

I voluntarily agree to cooperate in such investigation, and release from all liability or responsibility the State of Missouri, Office of Administration, Division of Facilities Management, Design & Construction, and all other persons, firms, corporations, and institutions supplying the above requested information.

I understand in the process of performing the requirements of the contract, the contractor and/or the contractor's personnel may become aware of information required by law to be kept confidential. Therefore, I agree I must not at any time disclose, directly or indirectly, any information gained during the performance of the janitorial services.

Signature	**Date**

Please return completed form and head shot photo for ID Badge to FMDCSecurity@oa.mo.gov.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes.

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;
b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION &
MISSOURI STATE HIGHWAY PATROL
CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the FBI CJIS Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the FBI CJIS Security Policy; (4) Title 28, Code of Federal Regulations, Part 20, (5) 576.050 RSMo; and (6) the MULES Policies & Procedures Manual, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____

Name of Contractor

_____ _____ _____

Printed Name & Signature of Contractor Employee Date

_____ _____ _____

Printed Name & Signature of Contractor Representative Date

Security Awareness Training

MSHP Information Security Unit

1. What is CJI?
   - CJI is criminal justice information
   - CJI is any information collected by FBI, MSHP and other criminal justice entities
   - It is available to anyone who is authorized to use CJIS systems – MULES, MoDEx, REJIS etc
   - CJI is not limited to criminal history or information available through MULES but can also include CAD, RMS, and MCD/MDT systems.
   - Includes PII (Personally Identifiable Information) and other derived information
   - This definition has changed from previous years – it is broader to include all information directly from state and federal systems but also data derived from those sources.

2. What is your responsibility?
   Information contained within and obtained from the CJIS Information Systems is sensitive information.
   Improper access, use, and dissemination of CJIS data is serious, and may result in the imposition of administrative sanctions including termination of services, as well as state/federal criminal penalties.

   YOUR RESPONSIBILITY IS TO PROTECT THE INFORMATION AND REPORT SECURITY INCIDENTS

3. What happens if you misuse CJI?
   Misuse of official information 576.050.
   - A person commits this crime if he or she knowingly obtains or recklessly discloses information from the Missouri uniform law enforcement system (MULES) or the National Crime Information Center System (NCIC), or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job.
   - Misuse of official information is a class A misdemeanor

4. Dissemination
   - Only use the information to perform your job duties
   - Do not disclose or share information with anyone that is not authorized to have access to the information i.e. the authorized individual/agency will have an agreement with your agency.
   - If releasing to another authorized agency that is not part of the agreement – a log must be kept of the dissemination

- Information needs to be protected from creation to destruction
- Be aware of where information could go if released

5. Why the big deal about protecting information?
   - In 2013 the average cost for the loss of a single record - $188
   - The average breach results in the loss of around 28,000 records
   - 28,000x$188.00=approximately $5.2 Million in damages for an average breach
   - Fines - $150,000 per incident
   - Indirect costs are even higher
   - Civil liabilities can be almost limitless
   - Loss of public confidence is the most damaging aspect for public safety

6. Who should you report security incidents to?
   Report your incidents to the TAC or LASO of your agency - they will report the incident to the appropriate people
   For Patrol employees, security incidents should be reported to the Patrol's Information Security Unit in the CJIS division at the contact information below:

   - MSHP Information Security Unit – email: cjissecurity@mshp.dps.mo.gov
     Phone: 573-522-3820

   CJIS Security Administrators
   - CSA - CJIS Systems Agency/ MSHP
   - CSO - CJIS Systems Officer/ Major Sarah Eberhard - MSHP
   - ISO - Information Security Officer/ Patrick Woods - MSHP
   - TAA -Terminal Agency Administrator/ Sheriff or Chief
   - TAC - Terminal Agency Coordinator/ Assigned at the MULES agency
   - LASO - Local Agency Security Officer/Assigned at agency with access to CJI

   Terminal Agency Coordinator (**TAC**) - The person in your agency responsible for the MULES computer system & operator access. They have the highest level of certification at your agency and must be a full-time employee. The TAC maintains MULES security for your agency's Computer Center

   Local Agency Security Officer (LASO)
   - Maintains list of users who have access to CJI
   - Identify how equipment is connected to MSHP
   - Ensures proper personnel screening procedures are being followed
     - Fingerprint check personnel that have unescorted access to secured locations
   - Ensure security measures are in place and working
   - Notify MSHP ISO of any security incidents at local agencies -
     MSHP Information Security Unit - email:cjissecurity@mshp.dps.mo.gov
     Phone: 573-522-3820

7. Incident Response Plan
   Definition of an incident - An incident is the act of violating an explicit or implied security policy.
   These include, but are not limited to:
   - attempts (either failed or successful) to gain unauthorized access to a system or its data
   - unwanted disruption or denial of service
   - the unauthorized use of a system for the processing or storage of data
   - changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

8. Security Incident Response Plan
   - The Security Incident Response Plan should be part of your agencies policies and procedures.
   - If you are suspicious of something, report it through your agencies procedures
   - It is better to have multiple false alarms than miss one incident
   - The plan extends to a threat against any CJI – not just computer related – also includes physical media

9. Media Protection
   - The protection must include both physical and electronic media
   - Electronic Media includes Flash Drives, Hard Drives, CD, DVDs
   - Physical Media includes documents, pictures, etc
   - All media must be stored in secure areas
   - Access to media should be granted to authorized personnel only
   - Make sure printed information is printed to the correct printer
   - All CJI data located, transmitted or transported outside a secure location must be encrypted, according to FBI standards, or carried in a locked container.
   - Physical media must also be protected in transit - it should be carried in locked container or folders where it is not visible to the public

10. Media Disposal
    - All CJI data must be properly disposed of
    - Electronic media must be physically destroyed or overwrite three times
    - Physical media must be shredded or incinerated
    - Put paper media in shredding bins
    - Give electronic media to your agency's IT staff

11. Physical Security
    - In order to handle or process CJI, staff and equipment must be in a secure location
    - The location could be a building, room, area

- Area must be marked
- List of authorized users must be maintained
- Must have controls such as locks to verify individual before granting access
- Computer and Information system equipment areas must also be secure locations
- Monitors and printers must be secure in order to prevent unauthorized viewing of CJI
- Visitor access must be controlled and logged in secure locations
- Visitors must be escorted and monitored at all times
- It is recommended visitor log is maintained
- Information systems related items (laptops, IPads, handhelds, etc) entering and exiting the area are recommended to be controlled or noted on visitor logs

12. Vulnerabilities
    Vulnerabilities are points in systems that are susceptible to attack.

    Vulnerabilities may include:
    - Physical
    - Natural
    - Media
    - Human
    - Communication
    - Hardware and Software

13. Threats
    - A threat is an unintentional or deliberate event or circumstance which could have an adverse impact on an information system. Threats can come from internal or external sources.
    - One way to think about threats vs. vulnerabilities vs. risk:
        - A hole in a roof is a **vulnerability**
        - The rain is a **threat**
        - **Risk** is determined by the forecast or how likely it is to rain
    - Just like in the example above, risk determines how severe the treat or vulnerability is to your environment, I.T. or otherwise.

14. Natural Threats
    Natural threats can endanger any facility or piece of equipment. You may not be able to prevent a natural disaster, but damage can be minimized with proper planning. Natural threats include:
    - Fire
    - Flood
    - Lightning
    - Power Failures

15. Unintentional Threats

Unintentional threats are actions that occur due to lack of knowledge or through carelessness. These threats can be prevented through awareness and training.

Unintentional threats include:

- Physical damage to equipment
- Deleting information
- Permitting unauthorized users to access information

16. Intentional Threats

Intentional threats are those threats that are deliberately designed to harm or manipulate an information system, its software and/or data. Security software such as an antivirus program is designed to protect against intentional threats.

Intentional threats include:

- Social Engineering
- Phishing
- Sabotage
- Eavesdropping
- Unauthorized data access
- Intrusions
- Denial of Service
- Theft

17. Acceptable Use Policy

This is a legal statement you agree to when you login to your computer or an application

- You should read it – it tells you what you can and cannot do
- Similar to the paper agreements you have signed
- This should be a part of sign on for all information systems

18. Password Policy

- Your agency's password policy should be:
- Minimum length of 8 characters
- Cannot be a dictionary word or proper name
- Cannot be user id
- Will expire every 90 days
- Cannot be identical to previous 10 passwords
- Cannot be transmitted in the clear
- Cannot be displayed when entered
- Do not share with anyone (including your agency IT staff)
- Do not write down
- Try not to increment numbers in the password
- Make it easy to type or user keyboard patterns

Hints for good passwords:

- Use phrases or run words together
- Substitute special characters for common letters
- $0methingeasy2remember

19. Malicious Code
    - Malicious code includes viruses, malware, spyware and other code that is part of the code on a machine that does not fit into the standard configuration
    - Can be loaded intentionally or unintentionally
    - Malicious is anything that could potentially disrupt the normal processing of a computer system.
    - Be careful of websites or applications that ask to load software on your machine.
    - Something as non-threatening as a weather notification tool could be used as an attack vector
    - Unknown and un-patched software could be exploited
    - If you need software to perform your job duties – contact your supervisor or agency IT staff to help you install the software.

20. Email/Email Attachments
    - Email is NOT a secure method of communication except within LEO or MSHP (LAN)
    - As a general rule, don't send anything in an email you don't want others to see
    - Do not send CJI information in an email unless you know the proper technical controls are in place – encryption and access control
    - All email should be scanned for known viruses and spam but it is still an easy avenue for malicious code
    - Virus/Spam detection is only as effective as the latest update
    - You are the last defense in protecting our environment
    - Do not respond or open emails from unknown senders
    - If something doesn't look right, it probably isn't legitimate

21. Internet Policy
    - Internet should be monitored and controlled
    - All devices that connect to the Internet should be protected by a firewall

22. Social Engineering
    - Social engineering is the attempt to gather information by deception
    - Scams and phishing attempts are the major categories of social engineering
    - Social engineering could come from any source – email, telephone, face to face.
    - It won't be obvious the person is trying to gather information
    - Could be masked as a marketing call
    - If you are suspicious – do not answer – report the incident
    - Never respond to an email asking for personal or confidential information, especially if it comes from someone you do not know

23. Laptop/Handheld/Personal Devices
    - There are many personal and work related devices available - know your agency's policy on using these devices
    - Personal devices are not allowed to access CJI Systems
    - Devices need to be secure and managed by the agency's IT staff
    - Need to be password protected and encrypted
    - If lost or stolen, report it as an incident
    - Laptops must be encrypted
    - Laptops/desktops will be managed by IT department to ensure proper controls are in place
    - Agency equipment should not be used for personal uses
    - Do not load unapproved software on any devices
    - Be aware of screen location – avoid shoulder surfing – use screen savers when possible
    - Lock computer before stepping away
    - Use of personal equipment is not allowed to connect to CJIS networks
    - CJI information shall not be stored, accessed or viewed from personal computing equipment
    - CJI information shall not be accessed from library, school or hotel computers

24. Access Requests
    - The access request process should be a documented process
    - The main focus is separation of duties and least privileged access
    - A person who authorizes access should not have the ability to implement the request
    - The level of access should be enough to perform the job duties - do not give higher authority unless needed
    - If your user id is compromised, if you have least level of access, the less information is at risk
25. Mobile devices
    - Devices cannot be “rooted” or “jailbroken”
    - CJI is only to be transferred between CJI authorized applications on the device
    - Report if the device is lost, stolen, or compromised
      - Include the lock state of the device
      - Include if there are capabilities for remote tracking or wiping of the device
    - Must have a password to unlock the device

Summary

- Information needs to be protected from creation to destruction
- Be aware of information flow – be aware of whom you provide information to - you may pass it to a legitimate person but they may not understand the policy and pass the information to others who are not authorized to have the information
- Providing too much information may allow misuses of the information
- Make every reasonable effort to protect the information you have access to
- Protect the information systems equipment you work with

- Report computer security incidents immediately - containment is easier during the initial stages
- Be aware of who is asking for information

Noncompliance

Misuse of official information. 576.050.

A person commits this crime if he or she knowingly obtains or recklessly discloses information from the Missouri uniform law enforcement system (MULES) or the National Crime Information Center System (NCIC), or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job.

Misuse of official information is a class A misdemeanor

I agree that I have read the Security Awareness Training material that was provided to me. I understand what I have read and I do not have any questions. I agree to abide by the rules and regulations as outlined in the Security Awareness Training material.

_____ _____

Signature Date

_____

Printed Name

_____ _____

Agency Name ORI

MISSOURI STATE HIGHWAY PATROL

SEXUAL HARASSMENT ADVISORY FOR EMPLOYEES / STUDENT INTERNS

Do you understand what sexual harassment is?
When a person in a position of authority in your workplace requires you to submit to sexually offensive actions, relations, or situations as a condition of employment or as a basis for employment decisions (assignments, promotions, etc.), that is called **quid pro quo** sexual harassment.

When unwelcome conduct of a sexual nature by members of management, supervisors, co-workers, or persons who are not employees but with whom you must associate in performing your job unreasonably interferes with your job performance or creates an intimidating, demeaning, abusive, or offensive workplace, that is called sexual harassment through a **hostile work environment.** Saying you are not qualified for your job just because of your gender is also improper.

Do you understand your rights about past situations?
Just because you may have kept silent about offensive conduct in the past you still have a right to object to and/or report that conduct. You are, however, strongly encouraged to promptly report all such instances. If you participated in certain types of conduct in the past, e.g., telling dirty jokes, but no longer want to do so, you have a duty to tell the person(s) with whom you did that activity that you no longer want to do so.

Do you know what constitutes sexual harassment?
Either quid pro quo harassment or a hostile work environment whether it is directed toward a male or female. See General Order 26-06 for a detailed explanation and a list of examples. If you ever have questions, refer to the order and/or ask your supervisor or commander.

Do you know how to deal with sexual harassment as a victim?
What you should do is explained in General Order 26-06. Basically, tell the offending person(s) that their actions are unwelcome and offensive and should be stopped immediately. While some people may prefer to handle the situation themselves, employees are **strongly encouraged** to officially report **all** instances of sexual harassment - to their supervisor, commander, or directly to the Professional Standards Division.

Do you know what you should do if you witness sexual harassment?
Employees who see or hear what **appears** to be sexual harassment should, at least, inform their supervisor or commander. They may submit a Complaint Receipt, SHP-872, detailing the alleged misconduct.

Are you aware that retaliation against those who report sexual harassment is prohibited?
General Order 26-06 prohibits retaliation against anyone for reporting sexual harassment or for participating in an investigation of sexual harassment. Supervisors and managers of employees who have reported sexual harassment have to watch for and keep in touch with the employee to make sure no retaliation occurs.

I have personally read General Order 26-06 and have had the opportunity to ask my supervisor any questions I have related to it. I have a thorough understanding of General Order 26-06, as well as my rights, duties, and responsibilities related to sexual harassment.

Employee's / Intern's Signature	Printed Name	Date

Reviewing Supervisor's Signature	Printed Name	Date

MISSOURI STATE HIGHWAY PATROL
GENERAL ORDER

Subject		Number
SEXUAL HARASSMENT		**26-06-1744**
Date of Issue	Effective Date	Distribution
March 1, 2018	**March 12, 2018**	**A**

Related Directives/Forms
Section 703, Title VII, of the 1964 Civil Rights Act; General Orders 26-01, 26-02, and 52-01; Intradepartmental Correspondence, SHP-15; Counseling Report, SHP-78; Sexual Harassment Advisory, SHP-356; Complaint Receipt, SHP-872

Instructions
Discard Rescinded General Order 26-06-1482

PURPOSE: To prohibit all forms of sexual harassment and establish procedures to report and investigate allegations of sexual harassment to facilitate timely, appropriate corrective action.

POLICY: To maintain a professional work environment free of sexual harassment, by preventing sexual harassment, taking direct, immediate action to report, investigate, and remedy all instances which may occur, and by not tolerating sexual harassment in any form or at any level.

Std 26.1.1 (Distr "A") & 26.1.3 -Entire Order

DEFINITIONS:

1. **Sexual Harassment:** Harassment on the basis of sex is a violation of Section 703 of Title VII of the Civil Rights Act of 1964. Unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when:

   a. Submission to such conduct is explicitly or implicitly made a term or condition of an individual's employment.

   b. Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual.

   c. Such conduct creates a hostile work environment.

2. **Workplace:** Any place where Patrol work or activities are performed or there is a work-related context including work-related discussions or activities conducted at private residences, private business, during out-of-state business trips, etc.

I. FORMS OF SEXUAL HARASSMENT

A. Quid Pro Quo Harassment

Quid pro quo harassment occurs when a supervisor, member of management, or other person in a position of authority in a workplace requires an employee to submit to sexually offensive actions, relations, or situations as a condition of employment or as a basis for employment decisions. This also includes persons who are not employees, but who are working for the Patrol, e.g., National Guard personnel, student interns, independent contractors, etc. **Employees are prohibited from explicitly or implicitly engaging in Quid Pro Quo sexual harassment.** Examples include, but are not limited to:

1. An employee who appears uncomfortable with sexually explicit language in the workplace being told, "**That's the way we talk, get used to it if you want to keep working here**."

2. An employee being required to engage in sexual relations to remain eligible for a promotion, obtain a favorable job performance evaluation, or avoid possible disciplinary action or dismissal.

B. Hostile Work Environment

1. Hostile work environment harassment exists when unwelcome conduct of a sexual nature unreasonably interferes with an employee's job performance or creates an intimidating, demeaning, abusive, or offensive work environment. A hostile work environment can cause an adverse psychological or emotional effect upon an employee. **Employees are prohibited from engaging in any form of sexual harassment that creates a hostile work environment for any person.**

2. A hostile work environment can be created by members of management, supervisors, co-workers, or persons who are not employees but with whom the affected individual must associate in performing job-related duties. A hostile work environment may be created when:

   a. The offensive conduct is not specifically directed toward the offended employee. Third party exposure to offensive conduct, such as overhearing sexually explicit discussions or jokes, seeing sexually explicit photographs or conduct by others can create a hostile work environment.

   b. It is stated or inferred that an employee is not competent or qualified for an assignment due to gender, or that persons should be restricted to traditional roles for their gender.

II. ROLES AND CIRCUMSTANCES

A. Gender of Involved Parties

Both males and females can be sexually harassed, or sexually harass others.

B. Prior Submission

Employees who have previously been subjected to any form of sexual harassment but did not object or file a complaint, are not barred from objecting or filing a complaint for similar conduct in the future. Employees are, however, strongly encouraged to promptly report all such instances.

C. Participation or Consent

In those situations in which employees have voluntarily participated in behavior of a sexual nature, speech, conduct, or a consensual relationship, but no longer welcome such behavior, those employees have an affirmative duty to declare to the person(s) with whom the employee has engaged in such activity that the behavior is no longer welcome.

III. PROBLEMATIC AND PROHIBITED BEHAVIOR

A. General Prohibitions

No employee will create an intimidating, hostile, or offensive environment, or subject any person to sexually offensive conduct or sexual harassment through verbal, nonverbal, or physical behavior of a sexual nature. In determining whether alleged conduct constitutes sexual harassment, the Patrol will look at the totality of the circumstances, such as the nature of the incident(s) and the context in which the alleged incident(s) occurred. The determination of the legality of a particular action will be made from the facts, on a case-by-case basis.

B. Behavior Always Prohibited as Sexual Harassment

The following prohibited activities always constitute sexual harassment:

1. Making acceptance of unwelcome sexual conduct or advances or requests for sexual favors a condition of employment, continued employment or promotion, or any other employment decision.

2. Unwelcome sexual advances or overtures, or unwelcome teasing of a sexual nature.

3. Intimidating another person, directly or indirectly (to include communication such as e-mail, or written or recorded messages), for not complying with sexual advances/overtures.

4. Sabotaging the efforts of an employee so as to be able to ridicule that person for an apparent inability to properly perform the job because of gender.

C. Prohibited Behavior Subject to Determination

The following activities are prohibited and depending on the context and circumstances, may be determined to be sexual harassment:

1. Telling stories or jokes or making comments or innuendoes having a sexual connotation.

2. Unwelcome kissing, hugging, or unnecessarily touching, brushing, or bumping against a person.

3. Displaying or circulating by any medium within the workplace pictures, posters, calendars, drawings, pin-ups, cartoons, or similar publications of nude or scantily clad persons.

4. Displaying or circulating by any medium within the workplace written or electronic materials, pictures, drawings, or other similar materials which are sexually suggestive or have a sexual connotation.

5. Repeatedly asking an employee out, unnecessarily following an employee, making unwelcome telephone calls, sending unwelcome electronic or personal messages or items, making unnecessary and unwelcome personal visits or contacts, or intimidating another person.

6. Making suggestive or sexually offensive gestures, facial expressions, or movements.

7. Suggestive or demeaning staring or looks such as leering, ogling, and "visually undressing."

8. Referring to others using demeaning or inappropriate terms such as honey, hunk, sweetie, babe, girls, doll, etc.

9. Telling or suggesting to members of the opposite sex that they are not competent or qualified for an assignment due to gender.

10. Making comments or asking questions of a vulgar, provocative, sexually derogatory, or suggestive nature, e.g., discussing sexual activities, commenting about a person's body, commenting about how an employee's clothing fits, etc.

11. Discussing another employee's personal relationships or sexual activities or spreading rumors or lies about others.

12. Discriminating based upon gender by failing to provide equal opportunity in the workplace. Discrimination includes disparity or unfavorable treatment or employment decisions regarding any person or group of persons in comparison to other persons or groups because of their gender.

D. Retaliation Prohibited

No employee will retaliate against any person for reporting instances of perceived sexual harassment or for participating in any manner in an investigation of allegations of sexual harassment.

IV. FACTORS AND CIRCUMSTANCES

A. Frequency of Offensive Behavior

A single substantiated incident of certain behaviors may constitute sexual harassment, while a pattern of such behavior constitutes sexual harassment in most cases.

B. Context of Behavior

All allegations of sexual harassment will be analyzed by the nature of the conduct, the context in which the incident behavior took place, the perspective of each party involved, and the totality of the circumstances. Courts have established that the "reasonableness standard" in determining the severity and pervasiveness of sexual harassment is gender specific and will be determined from the perspective of the person who found the conduct offensive.

C. Duty Status

While sexual harassment under Title VII deals with the workplace, the prohibited acts that constitute sexual harassment can be committed while one or more of the parties involved is not "on duty." **All such acts ultimately have an adverse effect upon the workplace; therefore, any such conduct is specifically prohibited regardless of the duty status of either individual**.

V. RESPONSE TO HARASSING BEHAVIOR

A. Employees Subjected to Harassment

1. Employees who believe they are being subjected to sexual harassment should, **if feasible**, inform the person committing the conduct that the actions are unwelcome and offensive and should be stopped immediately. If the person does not immediately stop the offensive behavior, the employee should promptly contact the appropriate supervisor for assistance.

2. It is recognized that some persons may prefer to deal with some incidents of offensive behavior themselves without reporting the incident to a supervisor and filing a formal complaint. Because the Patrol has an obligation to prevent, investigate, and correct sexual harassment, employees are **strongly encouraged** to officially report **all** instances of sexual harassment as outlined in this order.

B. Employees Witnessing Suspected Harassment

Employees who observe conduct that appears to constitute sexual harassment should, at a minimum, inform their supervisor of their observations or submit a Complaint Receipt, SHP-872, detailing the alleged misconduct.

VI. REPORTING SEXUAL HARASSMENT

A. Consultation with Supervisor

1. Employees who believe they have been subjected to sexual harassment should promptly report the incident to their supervisor and complete a Complaint Receipt, SHP-872. All circumstances and a listing of any witnesses to the incident should be thoroughly documented on the complaint form.

2. Supervisors receiving reports from employees who believe they have been sexually harassed will forward those complaints **in all cases** to their commander, regardless of the supervisor's personal beliefs about the incident.

3. If the employee's supervisor is involved in the incident, the employee may go to the next level in the chain of command or report the incident directly to the Professional Standards Division.

B. Form

Sexual harassment is misconduct; therefore, employees will report sexual harassment in accordance with General Order 52-01, “Complaint Reporting and Internal Investigations." After reviewing the facts and circumstances stated in the complaint, the director of the Professional Standards Division may recommend the employee file a grievance or take other appropriate action if no factual allegations of misconduct are alleged in the complaint.

VII. INVESTIGATIONS AND CONFIDENTIALITY

A. Roles

1. The Professional Standards Division will be promptly contacted and have primary jurisdiction in investigating all allegations of sexual harassment.

2. Individual components will not conduct internal investigations of sexual harassment unless so authorized by the director of the Professional Standards Division.

B. Confidentiality

All employees will observe strict confidentiality with respect to sexual harassment incidents and investigations. Information will be shared only with those who specifically need to know of the incident or to fulfill legal requirements, Patrol responsibilities, and policy requirements.

C. Conduct

Investigations of sexual harassment will be conducted as outlined in General Order 52-01 and will be conducted in a thorough, prompt, discreet, and sensitive manner. The Professional Standards Division will develop and maintain a detailed policy regarding such investigations to ensure they are properly conducted. This provision will not apply to situations arising out of enforcement contacts with offensive subjects.

VIII. SUPERVISORY RESPONSIBILITIES

A. Prevention of Sexual Harassment

Supervisors, including all managerial personnel, are responsible for preventing sexual harassment in the workplace. In substantiated cases of repeated or flagrant sexual harassment within a particular component, a separate internal investigation will be conducted of the component supervisor for possible malfeasance of duty.

B. Knowledge of Harassment and Procedures

Supervisors and managers will be knowledgeable regarding the various acts and types of conduct that may constitute sexual harassment and the procedures for reporting incidents of sexual harassment. They will assist any employee who comes to them for help in resolving and reporting sexual harassment.

C. Lead by Example

Supervisors and managers will set a positive example in their personal speech and conduct to demonstrate to all employees in their component a true commitment against sexual harassment.

D. Observation, Intervention, and Prevention

Supervisors and managers will be continually alert for conduct by or affecting employees which could constitute sexual harassment, and will intervene and take appropriate action to stop subtle behaviors or practices in the workplace which could likely lead to sexual harassment allegations. A Counseling Report, SHP-78, will be completed to document corrective actions taken.

E. Action to be Taken

1. Supervisors and managers will take immediate action to stop, correct, and report all allegations or instances of sexual harassment about which they have knowledge regardless of whether the employees are assigned to their component.

2. If an employee who has been subjected to sexual harassment is unwilling to sign a Complaint Receipt alleging sexual harassment, and the supervisor has reasonable grounds to believe sexual harassment took place, the supervisor will submit a detailed Complaint Receipt form through channels to the Professional Standards Division.

3. Failure by supervisory and management personnel to take appropriate action will be grounds for discipline.

F. Prevention of Retaliation

Supervisors and managers of employees who have initiated allegations of sexual harassment will monitor activities in the workplace and periodically consult with the employee to ensure no retaliation against the employee occurs.

G. Sexual Harassment by Non-employees

1. Employees who, incident to their employment with the Patrol, are sexually harassed by persons who are not Patrol employees should report the situation to the affected supervisor.

2. Supervisors receiving reports of sexual harassment of employees by persons who are not Patrol employees will take action to ensure the harassment stops. The supervisor may personally contact the offending party to resolve the situation or may request assistance from a more appropriate Patrol

official. In all cases, the supervisor will submit Intradepartmental Correspondence reporting in detail the situation, the action taken, and the results obtained.

H. Limit Contact

Upon learning of allegations of sexual harassment within their component, supervisors will take immediate action to limit contact between the complaining and the offending party.

1. The action taken should be done with due consideration for work needs, the feelings of those involved, and possible adverse perceptions of others in the workplace.

2. Any accommodations should be to facilitate a professional and productive workplace and not to cause any person to feel as if the action is retaliatory or punitive.

IX. DISCIPLINARY ACTION

Disciplinary action, up to and including dismissal, will be taken against employees who violate this sexual harassment policy.

X. OFFENSIVE JOB-RELATED DUTIES

A. Exposure Inherent to Some Duties

In the normal course of performing their required duties, members and civilian employees may be exposed to sexually offensive conduct or materials resulting solely from the adverse nature of law enforcement work, contact with the public, and the related processing of reports and property.

B. Advance Notice to be Given

The Human Resources Division will inform persons seeking employment in jobs that could reasonably be expected to involve regular exposure to sexually offensive conduct or materials of this possibility either on the job posting notice, at the oral interview, in the job description, or through other appropriate means prior to hiring.

C. Supervisory

When feasible, supervisors will attempt to minimize the exposure of employees under their supervision to job-related sexually offensive conduct or materials.

Std 26.1.1- Item XI

XI. ADVISORY FORMS

A. New Civilian Employees or Interns

1. General Headquarters

a. The Human Resources Division orientation representative will review this order on sexual harassment with all new civilian employees hired in General Headquarters as part of the new employee orientation and with all new General Headquarters interns at the start of their internships.

b. On or about the first day of employment at General Headquarters, the immediate supervisor of each new employee or intern will review the Patrol sexual harassment policy with the employee or intern, including the fact that the policy will be available to the employee or intern at all times in the operations manual maintained in their workplace. The review will be done using the Sexual Harassment Advisory, SHP-356. Upon completing the review, the employee or intern and supervisor will sign and date the form.

2. Troops

a. This order on sexual harassment will be reviewed with all interns starting at the troop and with all new civilian employees hired at the troop level as part of the new employee orientation conducted by the troop.

b. On or about the first day of an internship or employment at a troop, the immediate supervisor of the intern or new employee will review the Patrol sexual harassment policy with the intern or employee,

including the fact that the policy will be available to the employee or intern at all times in the operations manual maintained in their workplace. The review will be done using the Sexual Harassment Advisory, SHP-356. Upon completing the review, the employee or intern and supervisor will sign and date the form.

B. Recruits

The Training Division will ensure this policy is reviewed with all recruits at the beginning of recruit training and ensure each recruit is issued a copy of this directive. After reviewing this order, the Training Division will have each recruit complete a Sexual Harassment Advisory, SHP-356.

C. Newly-Assigned Probationary Troopers

Troop commanders will ensure all newly-assigned probationary troopers review and sign a Sexual Harassment Advisory, SHP-356, on their first day in the troop following graduation from the Academy.

D. Newly-Promoted Supervisors or Newly-Designated Supervisors

All employees promoted and assigned to supervisory positions in their components will review and sign the Sexual Harassment Advisory, SHP-356, within two weeks of being promoted and assigned as a supervisor. This requirement applies to every newly-promoted and every newly-designated supervisory employee below that of troop commander or division director, regardless of their previously held rank or position. All newly promoted members below the rank of captain, regardless of any supervisory responsibilities, will review and sign the Sexual Harassment Advisory, SHP-356, within two weeks of being promoted.

E. Routing and Disposition of Advisory Forms

1. Human Resources (original)

All original Sexual Harassment Advisory forms required by this order will be promptly submitted to the Human Resources Division where they will be permanently maintained in the employee's personnel file.

2. Component (copy)

Copies of newly-signed Sexual Harassment Advisory forms required by this order will be retained by the component to facilitate verification of their completion.

F. Verification

In January of each year, the Human Resources Division will send a reminder to all troop commanders and division directors to verify Sexual Harassment Advisory forms required by this order are on file for all component employees. Troop commanders and division directors will submit an Intradepartmental Correspondence, SHP-15, through channels to the superintendent by March 1 of each year, acknowledging compliance.

XII. SUPERVISORY AND MANAGERIAL TRAINING

The Training Division will provide a block of instruction on the subject of sexual harassment in all Patrol supervisory and managerial training courses offered at the Academy.

Sandra K. Karsten

SANDRA K. KARSTEN, Colonel
Superintendent