



SBC Forensics

Policy and Procedure Manual

Effective Date: 4/5/2026

1430 Oak Court, Suite 308A Beaver Creek, Ohio 45430



1430 Oak Court, Suite 308A
Beavercreek, OH 45430
Telephone: 1.866.419.7263
Fax: 1.866.444.7263
www.sbcforensics.com

Table of Contents

**Policy
and
Procedure
Manual**

Policy and Procedure Manual

Shift Changes, Coverage, and Shift Exchange Policy

Policy: SBC Forensics requires employees assigned to scheduled shifts, on-call coverage, or other work assignments to remain responsible for those commitments unless an approved change has been arranged.

Employees requesting schedule changes are expected to take reasonable steps to secure qualified internal coverage through another approved SBC Forensics forensic examiner.

Purpose: To maintain uninterrupted patient coverage, ensure fair scheduling practices, minimize last-minute disruptions, and clarify employee responsibility for shift changes and coverage requests.

Scope: This policy applies to:

- Scheduled shifts
- On-call assignments
- Holiday shifts
- Weekend assignments
- Partial shifts
- Coverage swaps or trades
- Emergency replacement requests

Employee Responsibility

Once a shift or on-call assignment is posted, accepted, or assigned, the employee remains responsible for that shift unless a replacement has been approved by management.

Whether notice is given weeks in advance or last minute, the employee requesting the change is expected to make reasonable efforts to find qualified internal coverage.

This may include contacting other approved SBC Forensics forensic examiners to request:

- Full shift coverage
- Partial shift coverage
- Shift trades
- On-call swaps
- Mutual exchanges at a later date

Shift Trades / Exchanges

Employees may mutually agree to trade shifts or assignments, subject to organizational approval.

All trades must:

- Involve qualified and approved personnel with SBC Forensics
- Maintain required staffing coverage
- Comply with scheduling, credentialing, and fatigue considerations
- Be communicated to the Administrative Team promptly
- Receive final approval before becoming effective

Until approval is granted, the originally scheduled employee remains responsible for the shift.

Last-Minute Changes

Unexpected emergencies may occur. Employees needing same-day or short-notice coverage must notify the Administrative Team as soon as reasonably possible and continue assisting with coverage efforts unless unable to do so.

Management may assist with coverage attempts, but the employee remains responsible for timely notification and cooperation.

Uncovered Shifts / Failure to Report

Failure to obtain approved coverage, failure to report for an assigned shift, repeated schedule disruptions, or misuse of shift trade practices may result in corrective action.

Administrative Discretion

SBC Forensics reserves the right to:

- Approve or deny shift changes
- Reassign coverage as needed
- Limit excessive trades or repeated schedule changes
- Consider attendance history and operational needs
- Determine whether adequate effort was made to secure coverage
- Take corrective action when scheduling responsibilities are not met

Best Practice Expectations

Employees are encouraged to:

- Submit requests as early as possible
- Use professional communication when seeking trades

- Avoid excessive last-minute changes
- Confirm approvals before assuming a shift is covered
- Support coworkers through fair reciprocal scheduling practices

Est:4/5/2026

Policy and Procedure Manual

On-Call Shift Responsibilities and End-of-Shift Response Policy

Policy: Employees assigned to an on-call shift are fully responsible for responding to service requests for the **entire scheduled duration of the shift**.

An on-call assignment remains active **until the scheduled shift end time unless officially relieved by another qualified examiner or otherwise directed by the Administrative Team**.

Employees are **expected** to accept and respond to any case, dispatch, or assignment received at any time during their scheduled shift, including requests received immediately before the scheduled end of the shift.

Purpose: To ensure uninterrupted forensic coverage, timely patient response, clear employee expectations, and proper understanding of on-call obligations.

Scope: This policy applies to:

- Scheduled response shifts
- Backup coverage assignments
- Holiday, weekend, and overnight on-call coverage
- Any shift requiring readiness to respond to cases
- On-call forensic examiner shifts

Definition of On-Call Status

When assigned an on-call shift, the employee is being compensated or scheduled to remain available to respond to cases during the entire assigned time period.

Being “near the end of shift” does **not** end the obligation to respond.

The employee remains on duty and responsible for case response until:

- The scheduled shift end time has passed **and** no assignment was received during the shift, or
- Responsibility has been transferred to another approved examiner, or
- Management provides other direction

End-of-Shift Case Requests

If a case request, page, dispatch, or assignment is received **before the scheduled shift end time**, the on-call examiner assigned to that shift is expected to respond.

Examples:

- Shift ends at 6:00 PM and case received at 5:58 PM → assigned examiner responds
- Shift ends at 6:00 PM and case received at 5:55 PM → assigned examiner responds
- Shift ends at 6:00 PM and case received at 5:59 PM → assigned examiner responds

This expectation applies even if the examination continues beyond the scheduled end of the shift.

Overtime / Extended Time Expectations

Because forensic examinations vary in length, employees may be required to work beyond scheduled shift hours when:

- A case is received during the assigned shift
- An active examination is in progress
- Documentation, evidence handling, or transfer duties remain incomplete
- Patient care or operational needs require continued involvement

Extended time may range from minutes to several hours depending on the circumstances of the case.

Active Cases Near Shift End

If the employee is already on an active case near shift end, the examiner is expected to complete duties appropriately unless otherwise relieved or directed by management.

Employees should not leave an active examination solely because the scheduled shift time has ended.

Coverage Transfer

Only the Administrative Team may approve transfer of a pending or active case to another examiner.

Employees may not independently decline a case, delay response, or assume the next shift will automatically take the assignment.

Professional Expectations

On-call staff are expected to:

- Remain reachable during the full shift
- Be fit for duty during the full shift
- Be prepared to travel and respond during the full shift

- Understand that shift end time is not a guaranteed release time if a case is received before the shift ends
- Communicate professionally with Dispatch and leadership

Failure to Respond

Failure to accept or respond to a case received during an assigned on-call shift, refusal to remain on an active case, abandonment of duties, or repeated misunderstanding of on-call obligations may result in corrective action.

Administrative Discretion

SBC Forensics reserves the right to determine:

- Which examiner responds to a case
- Whether a case was received during shift coverage
- Whether continued duty beyond shift end is required
- Whether reassignment is operationally appropriate
- Whether employee conduct violated this policy

Operational Standard

On-call shifts are coverage commitments, not fixed departure guarantees. Personnel assigned to the shift are responsible for patient response needs arising at any point during that scheduled coverage period.

Est:4/5/2026

Policy and Procedure Manual

Chain of Command Policy

Policy: SBC Forensics maintains a clear chain of command to promote efficient communication, timely decision-making, operational consistency, and appropriate resolution of employee questions, concerns, requests, and workplace issues.

Employees are expected to utilize the established reporting structure whenever reasonably possible.

Purpose: To define lines of authority and communication so operational matters are addressed at the appropriate level, leadership is informed efficiently, and issues are resolved in an organized and professional manner.

Organizational Chain of Command

Unless otherwise directed, the standard chain of command is:

1. **Forensic Examiner / Staff Member**
2. **Administrative Team**
3. **Administrative Team of Professional Development**
4. **President**

This structure may be adjusted by leadership based on staffing, urgency, availability, or business needs.

General Expectations

Employees are expected to direct routine matters to the appropriate level first before escalating to higher leadership, unless circumstances justify immediate escalation.

This includes, but is not limited to:

- Scheduling questions
- Shift coverage issues
- Payroll questions
- Supply or equipment concerns
- Routine policy questions
- Administrative requests
- Communication concerns
- General workplace issues

Level 1: Administrative Team

The Administrative Team is the primary point of contact for day-to-day operational matters, including:

- Scheduling and shift changes
- Dispatch concerns
- Coverage requests
- Timekeeping or payroll routing
- General employee questions
- Routine documentation issues
- Immediate operational needs

Employees should begin with the Administrative Team whenever practical.

Level 2: Administrative Team of Professional Development

Matters may be escalated to the Administrative Team of Professional Development when:

- Previous attempts at resolution were unsuccessful
- Guidance is needed regarding policy interpretation
- Training, education, competency, onboarding, or professional standards are involved
- Performance improvement or workflow development is needed
- The matter requires higher-level review

Level 3: President

Matters may be escalated to the President when:

- Significant operational concerns exist
- Serious employee relations issues arise
- Legal, financial, or strategic concerns are involved
- Previous levels have been exhausted or leadership review is necessary
- Immediate executive intervention is warranted

Situations Allowing Direct Escalation

Employees may bypass normal chain of command when immediate circumstances require urgent reporting, including:

- Patient safety concerns
- Illegal activity
- Harassment or discrimination complaints
- Serious misconduct
- Workplace violence or threats
- Significant compliance concerns

- Emergencies where timely action is required

In such cases, employees should contact any available leadership level immediately.

Professional Communication Standards

All communication through the chain of command must remain professional, respectful, and solution-focused.

Employees are expected to:

- Present accurate information
- Cooperate with follow-up requests
- Avoid gossip or unnecessary bypassing of reporting levels
- Allow reasonable time for review and response

Failure to Follow Chain of Command

Repeated failure to use appropriate communication channels, unnecessary circumvention of leadership structure, disruptive escalation, or refusal to follow reporting expectations may result in corrective action.

Administrative Authority

SBC Forensics reserves the right to modify reporting structures, assign temporary authority, redirect concerns, or determine the appropriate leadership level for any matter based on operational needs.

Policy and Procedure Manual

Staff Communication Policy

Policy: Establish staff expectations regarding internal and external agency communication.

Purpose: To ensure all employees understand communication standards, code of conduct expectations, and response requirements necessary for effective operations.

Procedure: All personnel are expected to maintain a working, charged smartphone device at all times to support communication with administration and other business needs. The device must allow real-time communication through:

- Telephone
- Email
- Text messaging
- Facsimile (as applicable)

While on-call, any page or text notification regarding an examination request must be acknowledged immediately. Staff are required to contact the Answering Service or requesting facility within **5 minutes** of receiving the notification to confirm receipt.

During an all-page/all-call circumstance, all forensic nursing personnel are expected to promptly notify administration of their availability to respond.

All SBC Forensics personnel must conduct themselves professionally at all times when communicating, including but not limited to:

- In person
- Telephone conversations
- Email
- Text messaging
- Paging notifications

Unprofessional communication may result in disciplinary action.

Communication Methods

1.A Routine Communication

Staff will utilize the secure messaging application **TigerConnect** for business-related communication whenever applicable.

All employees must:

- Keep TigerConnect installed on their smartphone at all times
- Maintain access to the application for consistent communication related to job duties

If an employee cannot be reached through TigerConnect, administration or answering service personnel may contact the employee via their personal mobile phone.

1.B Active Examinations / Urgent Situations

During active forensic examinations or urgent matters, staff must use **TigerConnect** to communicate with administration or the answering service.

Employees are strictly prohibited from using non-HIPAA compliant communication platforms or native messaging applications to discuss any business-related or protected information.

2. Communication Expectations

Personnel may receive communication from:

- Management Personnel
- Medical Administrative Team
- Law Enforcement
- Prosecutors
- Multidisciplinary team members

When related to job duties, these communications should be returned within the same business day or by the following business day.

3. Employee Information Updates

Employees may receive notifications through:

- Email
- Postal mail
- Employee Gateway postings

These communications may include:

- Policy updates
- Contact information changes
- Continuing education opportunities
- General job-related correspondence

All employees are responsible for notifying the Administrative Team or Administrative Personnel immediately of any changes to their contact information.

4. Email Correspondence

Employees are prohibited from using personal email accounts for business-related communication.

All organizational email communication must occur through the approved company email hosting system to ensure HIPAA-compliant encryption.

Employees may not configure company email accounts within native smartphone mail applications.

The only approved mobile email access method is through the **Virtru** application.

Est:4/5/2026

Policy and Procedure Manual

Confidentiality Policy

Policy: Establish confidentiality requirements for all SBC Forensics personnel regarding patient information, records, and communications.

Purpose: To protect each patient's right to privacy and confidentiality regarding all verbal, written, electronic, and photographic information related to their care.

Definitions: "Confidential" refers to any privileged or protected information obtained during patient care, including verbal, written, electronic, photographic, or recorded information at any stage of creation, use, storage, or transmission. "Authorized personnel" are representatives from regulatory agencies, accrediting bodies, peer review organizations, quality assurance bodies, or others legally authorized to access records.

Procedure: All patient-related information is considered strictly confidential, including but not limited to:

- Examination records and documentation
- Medical and forensic findings
- Patient demographic information
- Statistics containing protected information
- Verbal communications regarding care
- Photographs related to patient care or injuries
- Electronic records or communications
- Evidence collection documentation

Personnel may discuss patient care and medico-legal findings only with:

- The patient
- Medical personnel directly involved in the patient's care
- Other individuals specifically authorized by the patient or law

All staff must maintain HIPAA compliance in all communication methods, documentation practices, and handling of records.

Patient Consent for Information Sharing

At the patient's request, Forensic Examiners nurses may discuss care with family members or significant others who are present during treatment, provided the patient gives consent.

Written authorization must be obtained when required before discussing a case with:

- Law enforcement

- Criminal justice officials
- Advocates
- Other non-medical parties involved during treatment

Access to Records

Authorized personnel may review records when necessary for:

- Quality assurance
- Regulatory compliance
- Peer review
- Legal processes
- Continuity of patient care

Unauthorized individuals shall not be granted access to any patient records or forensic examination information.

This includes victim advocates, rape crisis advocates, and witness advocates unless disclosure is made directly by the patient or through proper legal authorization.

No patient information or records shall be released by staff to advocates without appropriate authorization.

Photography / Personal Device Restrictions

To protect patient privacy and HIPAA compliance:

- Personnel are strictly prohibited from taking photographs of patient information, medical records, forensic documentation, evidence forms, charts, computer screens, or any confidential materials using personal devices.
- Personnel may not store, retain, forward, text, email, upload, or otherwise keep any patient-related image or confidential information on personal phones, tablets, smartwatches, cameras, laptops, or other personal devices.
- Only organization-approved and authorized equipment may be used for clinical or forensic photography in accordance with policy.

Any unauthorized image capture, storage, or transmission of confidential information may result in immediate disciplinary action, up to and including termination.

Record Security

Patient care records shall be secured in the Medical Records department of the facility where the forensic examination occurred, in addition to any official SBC Forensics records.

SBC Forensics records will be released only to appropriate law enforcement agencies or authorized entities in accordance with:

- Ohio Department of Health Protocol

- Applicable HIPAA regulations
- Ohio Revised Code
- Organizational policy

Outside Agency Notification Restrictions

SBC Forensics personnel shall not independently contact or request response from third-party organizations to jointly respond to forensic calls from medical facilities.

This restriction helps protect confidentiality, particularly in:

- High-profile examinations
- Sensitive cases
- Cases requiring heightened privacy protections

If assistance from another outside organization is requested, the request must be initiated by the medical facility—not SBC Forensics personnel.

Permitted Mandatory Notifications

Personnel may contact outside agencies only when required by law, protocol, or policy, including:

- Law Enforcement
- Ohio Department of Health
- Adult Protective Services
- Children’s Protective Services
- Other mandatory reporting agencies required by law

Violations

Any personnel found in violation of this policy may be subject to disciplinary action up to and including immediate termination.

Personnel Disciplinary Action

Policy: To establish general guidelines regarding employee conduct, performance expectations, and potential corrective or disciplinary action for SBC Forensics personnel.

Purpose: To ensure personnel understand that compliance with organizational policies, professional standards, operational expectations, and applicable laws or regulations is required as a condition of employment or contractual service.

Procedure: All personnel are expected to perform their duties in a professional, timely, ethical, and competent manner. Failure to meet organizational expectations, maintain standards of conduct, follow policies or procedures, comply with legal or regulatory requirements, or otherwise act in the best interest of the organization may result in corrective action or discipline.

Conduct or performance concerns may include, but are not limited to:

- Failure to meet job responsibilities or performance expectations
- Attendance, scheduling, availability, or response issues
- Failure to complete required documentation or administrative duties
- Communication concerns or failure to respond appropriately
- Unprofessional conduct, behavior, judgment, or appearance
- Failure to attend required meetings, trainings, or educational requirements
- Violation of organizational policy, procedure, protocol, or directive
- Conduct inconsistent with patient care standards, confidentiality, safety, or legal requirements
- Misuse of organizational property, systems, or resources
- Any conduct determined by leadership to negatively impact operations, reputation, safety, morale, or service delivery

The organization reserves the right to determine whether conduct or performance concerns warrant corrective action.

Corrective Action Options

Depending on the nature, severity, frequency, or circumstances of the concern, corrective action may include one or more of the following. Corrective action is not required to follow any specific sequence or progressive order.

- Coaching or counseling
- Verbal warning
- Written warning or documentation
- Performance improvement measures
- Retraining or education requirements

- Temporary removal from specific duties or schedules
- Suspension
- Probationary status
- Final warning
- Termination of employment or contractual relationship
- Any other corrective measure deemed appropriate by leadership

Administrative Discretion

SBC Forensics reserves the right to determine:

- Whether discipline is appropriate
- The level of discipline imposed
- Whether immediate action is necessary
- Whether prior warnings are required
- Whether an employee may continue duties during review
- Whether restrictions or conditions will apply to continued service

Serious misconduct, repeated concerns, policy violations, safety risks, confidentiality breaches, insubordination, or conduct inconsistent with organizational standards may result in immediate suspension or termination.

Investigations

The organization may review, investigate, or evaluate reported concerns before determining appropriate action. Personnel are expected to cooperate fully with any internal review or investigation.

Failure to cooperate may result in disciplinary action.

Return of Organizational Property

Upon separation from employment or upon request, personnel must promptly return all organizational property, records, devices, credentials, equipment, and materials.

Failure to return organizational property may result in legal action or other remedies available to the organization.

Employment Status

Nothing in this policy alters at-will employment status where applicable. SBC Forensics retains the right to end the employment or contractor relationship at any time, with or without notice, and subject to applicable law.

Final Authority

All disciplinary and corrective action decisions are made at the discretion of organizational leadership.

Est:4/5/2026

Policy and Procedure Manual

Dress Code

Policy: To establish professional appearance standards all personnel

Purpose: To ensure staff present a professional, respectful, and appropriate image to patients, the public, healthcare facilities, law enforcement, courts, and all outside agencies when representing SBC Forensics.

Procedure: All personnel are expected to maintain a neat, clean, professional appearance appropriate to their role, work environment, and assigned duties.

Clothing must allow staff to safely perform job responsibilities while maintaining professionalism, infection control standards, and public confidence.

1. Forensic Nurses / Clinical Staff

When providing direct patient care, forensic nurses shall wear professional attire appropriate for a healthcare setting.

Acceptable attire may include:

- Business casual clothing
- Approved healthcare scrubs
- White lab coat or approved clinical outerwear
- Closed-toe shoes appropriate for clinical work
- Clean athletic shoes or professional footwear

Staff must wear organizational identification badges at all times while:

- Providing patient care
- Entering healthcare facilities
- Attending meetings
- Representing SBC Forensics in any professional capacity

Personnel should maintain appearance standards that support clinical safety, including securing hair or accessories when necessary.

2. Law Enforcement Liaison / Field Support Personnel

When performing liaison or field duties, staff shall wear attire designated or approved by the organization.

Acceptable attire may include:

- Issued apparel with organizational logo
- Khaki or professional casual pants
- Clean, neat, duty-appropriate footwear

3. Court Appearances / Professional Meetings

When providing expert testimony or attending meetings with courts, prosecutors, attorneys, law enforcement, hospitals, or outside agencies, personnel must wear professional business attire.

Examples include:

- Dress slacks
- Professional blouse, shirt, or jacket
- Dress shoes
- Conservative professional attire appropriate for legal or executive settings

Casual clothing, denim, scrubs, or attire inconsistent with a professional setting may be prohibited unless specifically approved by leadership.

4. Prohibited Attire

The following items are not appropriate while on duty or representing the organization:

- Torn, damaged, excessively worn, or unclean clothing
- Clothing that is revealing, excessively tight, transparent, or otherwise inappropriate
- Open-toe shoes where safety concerns exist
- Clothing with offensive, vulgar, or inappropriate language or images
- Clothing displaying political endorsements, campaign messaging, or unrelated promotional material
- Attire that interferes with job duties, safety, patient care, or professional image
- Any appearance deemed unprofessional or inconsistent with organizational standards

This list is not exhaustive.

5. Grooming and Hygiene

Personnel are expected to maintain appropriate personal hygiene and grooming standards consistent with a healthcare and professional environment.

Hair, jewelry, fragrance, and accessories should not interfere with safety, infection prevention, communication, or job performance.

6. Administrative Discretion

Leadership reserves the right to determine whether attire or appearance is appropriate for the role, setting, or circumstance and may require employees to change attire or correct appearance concerns.

Failure to comply with dress code expectations may result in corrective action.

Est: 4/5/2026

Policy and Procedure Manual

Equal Opportunity/Non-Discrimination Statement

- Policy:* SBC Forensics is committed to providing equal employment opportunity and nondiscriminatory access to services.
- Purpose:* To promote fair employment practices, an inclusive workplace, and equitable access to patient care services for all individuals served by the organization.
- Procedure:* SBC Forensics provides equal employment opportunities to all employees and applicants. Employment decisions, including recruitment, hiring, assignment, promotion, compensation, training, discipline, and termination, will be made without unlawful discrimination or harassment.

The organization does not discriminate on the basis of any protected characteristic under applicable federal, state, or local law, including but not limited to:

- Race
- Color
- Religion
- Sex
- Pregnancy
- Sexual orientation
- Gender identity or expression
- National origin
- Age
- Disability
- Veteran status
- Marital status
- Genetic information
- Political affiliation where protected by law
- Any other status protected by law

Equal Access to Services

SBC Forensics is equally committed to providing patient care services in a fair, respectful, and nondiscriminatory manner.

No individual seeking services shall be denied access or treated differently on the basis of any legally protected status.

All patients and community members will be treated with dignity, professionalism, compassion, and respect.

Accommodations

Reasonable accommodations will be considered for qualified applicants, employees, and patients in accordance with applicable law.

Reporting Concerns

Any employee, applicant, patient, or community member who believes they have experienced discrimination, harassment, or unequal treatment is encouraged to report the concern to organizational leadership for prompt review.

Retaliation for making a good-faith complaint or participating in an investigation is prohibited.

Compliance

This policy shall be administered in accordance with all applicable federal, state, and local nondiscrimination laws and regulations.

Est: 4/5/2026

Policy and Procedure Manual

Incident Reporting Procedures

Policy: To establish procedures for reporting workplace incidents, operational concerns, and other events requiring documentation.

Purpose: To ensure timely reporting, proper documentation, and appropriate follow-up for incidents affecting personnel, patients, operations, safety, compliance, or organizational interests.

Procedure: When an incident occurs, the involved employee or personnel member must notify administration as soon as reasonably possible following the event.

In addition to verbal or direct notification, an official incident report must be completed through the Employee Gateway within **24 hours** of the incident, unless otherwise directed by leadership.

Incident reports must be completed accurately, thoroughly, and in a timely manner.

Notification to administration does not replace the requirement to submit a written incident report when one is required.

Incidents Requiring Reporting

Incidents requiring documentation may include, but are not limited to:

- Workplace injuries or safety concerns
- Patient care concerns
- Issues involving staff, facilities, multidisciplinary team members, vendors, or outside agencies
- Chain of custody concerns or evidence handling issues
- Failure to report for an assignment or complete assigned duties
- Equipment loss, damage, or malfunction
- Confidentiality, privacy, or security concerns
- Vehicle incidents while conducting business duties
- Unprofessional conduct or behavioral concerns
- Operational disruptions or service delays
- Any unusual event, error, near miss, or concern identified by leadership

This list is not exhaustive.

Administrative Review

Submitted reports may be reviewed by leadership for investigation, corrective action, risk management, quality improvement, training, or compliance purposes.

Employees are expected to cooperate fully in any follow-up review.

Failure to Report

Failure to timely report an incident, failure to provide accurate information, or failure to complete required documentation may result in corrective action.

Administrative Discretion

Leadership reserves the right to require an incident report for any event deemed appropriate, regardless of whether it is specifically listed in this policy.

Est: 4/5/2026

Policy and Procedure Manual

Mission Statement

Purpose: SBC Forensics exists to provide prompt, compassionate, patient-centered medico-legal care through high-quality forensic examinations, evidence collection, treatment support, and professional advocacy for individuals impacted by violence and trauma.

We are committed to delivering services with dignity, professionalism, sensitivity, and respect while supporting patients, healthcare partners, and the justice system.

Scope: Services may include, but are not limited to:

- Medical forensic examinations
- Evidence and specimen collection
- Sexual assault examinations
- Domestic violence examinations
- Law enforcement-requested examinations
- Strangulation and related forensic assessments
- Expert witness testimony in legal proceedings
- Forensic consultation and professional education
- Community outreach, awareness, and prevention education

Primary Populations Served

SBC Forensics primarily serves patients presenting with concerns related to sexual assault, violence, abuse, or other forensic needs, in accordance with organizational capabilities and applicable protocols.

Availability of Services

SBC Forensics strives to maintain on-call forensic nursing coverage 24 hours per day, 7 days per week, with response expectations based on operational needs, staffing availability, contractual obligations, and clinical circumstances.

Level of Service

Our forensic nursing professionals are trained in evidence-based forensic practice and maintain education, competency, and credentialing consistent with applicable standards, regulatory requirements, and professional organizations.

Training and qualifications may include:

- Didactic forensic education

- Clinical and preceptor-based training
- Competency validation
- Ongoing continuing education
- Professional licensure and certifications

Credentialing bodies may include recognized forensic nursing and nursing regulatory organizations at the local, state, and national level.

Commitment

SBC Forensics is dedicated to excellence in patient care, professional integrity, and compassionate response during some of the most difficult moments in a patient's life.

Est: 4/5/2026

Policy and Procedure Manual

Examination Response Procedures

Policy: Establish response expectations for Forensic Examiners nurses assigned to forensic examinations.

Purpose: To ensure timely, efficient response to service requests from contracted facilities and uninterrupted patient care coverage.

Procedure: When a scheduled Forensic Examiners nurse is assigned to an on-call or scheduled shift, the nurse must remain available and reachable by mobile phone and approved communication platforms beginning **90 minutes prior to the start of the shift**.

This availability allows SBC Forensics Dispatch or administration to notify the nurse of the facility where they are expected to report at the beginning of the scheduled shift.

Staff may be assigned a case location prior to shift start and are expected to plan accordingly so they are prepared to **arrive at the assigned facility and begin the examination at the start of the scheduled shift**, rather than departing for the facility at shift start.

Dispatch Notification

SBC Forensics Dispatch may provide assignment details through phone call, TigerConnect, text alert, or other approved communication methods.

Information provided may include:

- Assigned facility or hospital
- Patient or case readiness status
- Return contact number
- Special instructions
- Other operational details relevant to the response

Acknowledgement Requirement

Nurses must acknowledge receipt of dispatch communication within **5 minutes** of notification unless otherwise directed.

Failure to acknowledge or remain reachable may result in reassignment or corrective action.

Response Expectations

Once assigned, the nurse is expected to report promptly to the designated facility and meet applicable response-time requirements for that location.

Response times, readiness, timeliness, and communication compliance may be monitored.

Examination Responsibilities

The responding nurse shall complete the forensic examination in accordance with:

- Ohio Protocol for Victims of Sexual Assault
- Applicable medical forensic standards
- SBC Forensics policies and procedures
- Organizational clinical protocols
- Applicable legal and regulatory requirements

Administrative Discretion

SBC Forensics reserves the right to adjust assignments, reporting locations, scheduling expectations, and response procedures based on staffing needs, patient volume, operational necessity, or emergency circumstances.

Est: 4/5/2026

Policy and Procedure Manual

Payroll Policy

- Policy:* To establish payroll procedures and payment expectations for all SBC Forensics personnel.
- Purpose:* To ensure payroll processes are clearly defined, consistently administered, and that employees understand pay schedules, holiday observances, and procedures for reporting payroll concerns.
- Procedure:* Forensic staff and other personnel will be compensated in accordance with their assigned position, employment classification, contract terms, and approved job description.

Payroll is processed on a bi-weekly basis (every two weeks), unless otherwise communicated.

Pay Period Schedule

The Administrative Team will provide the annual payroll schedule, including pay period dates and pay dates, to all personnel.

Current payroll schedules will also be made available through the company intranet, employee portal, or other designated communication platform.

Recognized Holiday Periods

Holiday scheduling, payroll processing timelines, or operational adjustments may be impacted by recognized holidays, including but not limited to:

- New Year's Eve
- New Year's Day
- Memorial Day
- Independence Day (July 4th)
- Labor Day
- Halloween
- Thanksgiving Day
- Day After Thanksgiving
- Christmas Eve
- Christmas Day

This list may be modified by the organization as needed.

Payroll Questions or Errors

Personnel are responsible for reviewing their pay statements and promptly reporting any suspected payroll discrepancies.

Questions regarding payroll, compensation, hours, or pay statements should be directed to the Administrative Team as soon as reasonably possible.

Payroll Corrections

If a payroll discrepancy is reported, the Administrative Team will review the concern and determine the appropriate resolution.

Corrections may include, but are not limited to:

- Adjustment on the next payroll cycle
- Supplemental correction payment
- Clarification of recorded hours or applicable pay items
- Other corrective action deemed appropriate

The timing and method of any correction will be determined by the organization based on payroll processing timelines, verification needs, and applicable requirements.

Administrative Discretion

SBC Forensics reserves the right to interpret and administer payroll procedures, schedules, corrections, and compensation processes in accordance with applicable law and organizational operations.

Est: 4/5/2026

Policy and Procedure Manual

Public Speaking and News Media Contact Policy

Policy: To establish standards for media contact, public statements, community speaking engagements, and social media activity involving SBC Forensics, its personnel, patients, partner agencies, or active cases.

Purpose: To ensure SBC Forensics is represented in a professional, accurate, and consistent manner, to protect patient confidentiality, to preserve cooperative relationships with healthcare and public safety partners, and to reduce legal, operational, and reputational risk.

Procedure: Only authorized representatives designated by the Administrative Team may speak on behalf of SBC Forensics.

No employee, contractor, volunteer, or representative may make public statements, release information, or represent organizational positions without prior approval.

1. News Media and Press Inquiries

All requests for comment or information from:

- News media
- Reporters
- Journalists
- Podcasters
- Documentary producers
- Online media outlets
- Bloggers or content creators

must be referred immediately to the Administrative Team.

Personnel shall not independently respond to media requests regarding:

- SBC Forensics operations
- Patients or examinations
- Law enforcement matters
- Criminal investigations
- Pending litigation
- Partner organizations
- Internal matters
- Any case-related issue

Unauthorized communication with any media may result in disciplinary action, up to and including termination.

2. Public Speaking / Training / Community Events

Employees must receive prior approval from the Administrative Team before participating in any speaking engagement, interview, presentation, training, panel, conference, webinar, podcast, or public event where they are representing, referencing, or associated with SBC Forensics.

This includes:

- Community education
- Hospital education
- In-services
- Professional lectures
- Advocacy events
- Public awareness campaigns

Outside compensation related to such activities must also receive prior approval when connected to the organization, role, or services.

3. Social Media and Online Conduct

Personnel may not use social media, livestreaming platforms, blogs, forums, podcasts, messaging apps, or other online platforms to post, discuss, criticize, disclose, record, or comment on matters involving:

- Active or past cases
- Patients
- Examinations
- Evidence
- Law enforcement activity
- Hospitals or facilities
- Partner agencies
- Internal operations
- Coworkers or leadership
- Confidential workplace matters
- Any information obtained through employment or service

This applies whether or not names are used, and includes indirect references, screenshots, photos, videos, “anonymous” posts, coded language, or details that could identify a person, case, agency, or event.

Personnel are strictly prohibited from livestreaming, recording, or broadcasting while engaged in work duties, on a case, inside a facility, or while representing SBC Forensics unless specifically authorized in writing.

4. Professional Conduct

Personnel are expected to maintain professional judgment online and offline. Conduct that damages working relationships, public trust, patient confidence, or the reputation of SBC Forensics may result in corrective action.

5. Confidentiality

Nothing in this policy limits or replaces confidentiality, HIPAA, privacy, or evidence-handling requirements. Personnel remain responsible for protecting all protected or sensitive information.

6. Violations

Violations of this policy may result in disciplinary action up to and including:

- Removal from assignments
- Suspension
- Termination
- Legal referral where applicable

7. Administrative Authority

The Administrative Team reserves the right to determine whether communications, postings, conduct, or outside activity violate this policy or are inconsistent with organizational standards.

Policy and Procedure Manual

Quality Improvement

Philosophy: SBC Forensics is committed to the continuous improvement of forensic nursing services, patient care, documentation quality, operational effectiveness, and professional standards.

This commitment supports the organization's mission and reflects a culture of accountability, excellence, and ongoing development.

Quality improvement is an ongoing process integrated into daily operations, decision-making, patient services, and professional practice.

Improvement priorities may be established annually or as needed based on:

- Organizational goals
- Patient and customer expectations
- Operational trends
- Regulatory requirements
- Risk management concerns
- Clinical outcomes
- Feedback from stakeholders

Action Plan

SBC Forensics may utilize quality assurance and quality improvement measures including, but not limited to, the following:

Personnel Competency and Qualifications

- Ongoing review of staff qualifications, training, certifications, and competencies
- Annual or periodic competency validation as determined by leadership
- Identification of additional education or training needs

Documentation and Chart Review

- Ongoing review of forensic examinations, records, and documentation
- Internal leadership review, peer review, or medical oversight review as appropriate
- Evaluation of documentation standards such as:
 - Timeliness
 - Accuracy

- Completeness
- Professional quality
- Photography quality
- Compliance with protocols
- Evidence handling standards

Where applicable, quality findings may be shared with partnering facilities through appropriate channels.

External Feedback

The organization may request or receive feedback from external stakeholders, including but not limited to:

- Law enforcement agencies
- Prosecutors
- Crime laboratories
- Advocacy partners
- Regulatory bodies
- Other multidisciplinary partners
- Healthcare facilities

Feedback may be used to identify opportunities for improvement.

Corrective and Preventive Actions

When concerns are identified, the organization may implement actions including:

- Coaching or education
- Process improvement measures
- Policy revision
- Additional training
- Individual performance review
- Written plans of correction
- Operational changes

Monitoring and Recordkeeping

SBC Forensics may maintain records of quality improvement activities, findings, recommendations, and corrective actions as deemed appropriate.

Continuous Improvement Commitment

Quality improvement is an ongoing responsibility shared by all personnel. Staff are expected to participate in organizational efforts to improve patient care, service delivery, professionalism, compliance, and operational excellence.

Administrative Authority

Leadership reserves the right to determine quality priorities, review methods, performance indicators, corrective actions, and improvement initiatives based on organizational needs.

Est: 4/5/2026

Policy and Procedure Manual

HIPPA Compliance

Policy: Health Insurance Portability and Accountability Act (HIPAA) Security Policy and Procedure

Purpose: The purpose of this document is to list the policies and procedures SBC Forensics has documented and follows to remain compliant with the Security part of HIPAA. This document is used as a set of statements and instructions for SBC Forensics's workforce to follow, and as a training guide.

Procedure: This document describes SBC Forensics's policies and procedures relative to the Security part of the Health Insurance Portability and Accounting Act (HIPAA) of 1996. By having this document in place, and exercising the steps required to implement required activities, SBC Forensics declares that it has made its best efforts to be compliant with the Security part of HIPAA, as it applies to SBC Forensics

Ownership and Revisions

The SBC Forensics HIPAA Compliance officer, who is responsible for revisions and updates, owns this document. This is a "living" document. Updates that are a result of new discoveries, such as changing regulations or processes, will be added as needed by the document owner listed on the Revision History dates at the end of this policy.

Conventions

This document uses the following conventions:

- References to other documents or to sections within a document are underlined.
- Tables appear in Arial font.

In addition to variable values, italic type indicates emphasis or a new term. Administrative Safeguards

SBC Forensics has implemented administrative policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

Risk Analysis and Management

SBC Forensics conducts accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its computer systems, on a regular basis. When SBC Forensics's Compliance Officer believes any risks exist, the Compliance Officer addresses each risk and completes a risk mitigation report.

SBC Forensics has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule. These measures are described in detail in Sections 3 and 4 of this document.

Sanction Policy

SBC Forensics will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures, as detailed in SBC Forensics's Code of Conduct, which is available for review in SBC Forensics's HIPAA Compliance policy and procedure.

Information System Activity Review, Login Monitoring

SBC Forensics has implemented the following procedure to regularly review records of information system activity:

1. The Compliance Officer reviews files contained on SBC Forensics's computers weekly.
2. Since SBC Forensics's computers are basic and do not have the capability of maintaining automated tracking logs, the Compliance Officer regularly monitors usage of SBC Forensics's computers by regularly observing employee access and conduct for inappropriate access.
3. Use of employee email and shared storage will be tracked and reviewed weekly by the Compliance Officer.

Assigned Security Responsibility

SBC Forensics has named its Compliance Officer as the security official who is responsible for the development and implementation of the policies and procedures required by this HIPAA Rule. The Compliance Officer is the SBC Forensics Administrative Team.

Workforce Security, Authorization, Supervision, Clearance Procedure

SBC Forensics's policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, to prevent those workforce members who do not have access from obtaining access to electronic protected health information, to authorize and/or supervise workforce members who work with electronic protected health information or in locations where it might be accessed, and to determine that the access of a workforce member to electronic protected health information is appropriate, are listed below:

1. All employees who are allowed access to PHI are assigned passwords by the Compliance Officer to SBC Forensics's computer systems and online Employee Gateway. Passwords are kept locked up and managed by the Compliance Officer during office hours.
2. Employees who do not have access cannot obtain access, as they do not have the passwords
3. Employees with access to PHI are trained in the importance of protecting electronic PHI.

4. The Compliance Officer determines what workforce members appropriately have access to PHI, based upon thorough review and understanding of SBC Forensics's PHI Policies and Procedures, which are contained in SBC Forensics's HIPAA Compliance policy.

Termination Procedures

When the employment of a workforce member ends, or should no longer have access to PHI as determined by the Compliance Officer, that workforce member's access to electronic PHI is terminated by removing his or her user ID from SBC Forensics's computers or online software and programs.

Security Awareness, Training and Reminders

SBC Forensics has security awareness and training program for all members of its workforce (including management). When implementing its HIPAA Compliance Manual, SBC Forensics performed training sessions from its HIPAA Security Compliance Policies and Procedures. During regular staff meetings, SBC Forensics informs its staff of periodic security updates.

Protection from Malicious Software

SBC Forensics's computers have anti-virus scanning software installed, and updates to this software are purchased and installed when available. This ensures that SBC Forensics reasonably guards against, detects and reports malicious software.

All confidential files will not be transmitted to any electronic devices that are not secured with encryption software deemed appropriate by the Compliance Officer. This includes employees personal devices of any kind.

Security Incident Procedures, Response and Reporting

SBC Forensics's Compliance Officer notes any security issues he/she is aware of in the practice's Compliance Officer Incident Log, contained in SBC Forensics's HIPAA Compliance Manual, and addresses them on a case-by-case basis.

Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions

SBC Forensics backs up its computer systems nightly to a Compact Disk (CD) or peripheral data storage unit. The Compliance Manager secures the CD or storage unit to a safe, location nightly. Should an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) damage SBC Forensics's systems that contain electronic protected health information, the Compliance Officer (or designated representative) takes the backup copy of the patient data, along with the original CDs of SBC Forensics's software to a reputable computer service company, and restores the system to its last operational state. The Compliance Officer (or designated representative) operates SBC Forensics's systems from that location until the disaster situation is remedied.

SBC Forensics's Compliance Officer tests this procedure any time new software programs are installed on SBC Forensics's computer, to ensure data can be backed up, restored and operational as soon as possible.

Evaluation

SBC Forensics 's Compliance Officer performs a technical and non-technical evaluation of the procedures in this document quarterly, or any time there are significant environmental or operational changes affecting the security of electronic protected health information.

Business Associate Contracts and Other Arrangements

SBC Forensics has contractual agreements in place with its business associates who create, receive, maintain, or transmit electronic protected health information on our behalf, which gives us satisfactory assurances that the business associate will appropriately safeguard the information. We realize that this standard does not apply with respect to:

1. Transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual;
2. Transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the relevant HIPAA requirements apply and are met; or
3. Transmission of electronic protected health information from or to other agencies providing the services when the covered entity is a health plan that is a government program providing public benefits, if the relevant HIPAA requirements are met.

Physical Safeguards

SBC Forensics has implemented physical safeguard-related policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

Facility Access Controls

SBC Forensics has implemented the following policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed:

1. SBC Forensics's computers are kept encrypted at all times.
2. Software, email and data storage for PHI are kept encrypted at all times.
3. Only personnel requiring access to these systems are authorized to use them.

Contingency Operations

SBC Forensics has established procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. See Section 2.10, Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions, for details.

Facility Security Plan

SBC Forensics has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Computers are kept in secure locations and encryption software remains updated at all times.

Access Control and Validation Procedures

SBC Forensics has implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. The Compliance Officer oversees access to facilities and computers.

Maintenance Records

SBC Forensics has implemented policies and procedures to document repairs and modifications to the physical components of its facility, related to security. The Compliance Officer ensures, on a daily basis, that the physical facility is in working order and documents any deficiencies for follow-up and repair.

Workstation Use

SBC Forensics has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of its specific workstation or class of workstation that can access electronic protected health information. Only personnel requiring access to these systems are authorized to use them.

Accountability

The Compliance Officer maintains a record of the movements of hardware and electronic media and any person responsible therefore.

Data Backup and Storage

The Compliance Officer or designated authorized representative creates a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Physical safeguards

SBC Forensics has implemented technical safeguard-related policies and procedures in the following areas to prevent, detect, contain, and correct security violations, as described in the following sections.

Access Control

SBC Forensics has implemented technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. See Section 3.4, Access Control and Validation Procedures, for details.

Unique User Identification

SBC Forensics assigns a unique name and/ or number for identifying and tracking user identities by setting up login IDs and passwords to each employee, as applicable.

Emergency Access Procedure

SBC Forensics has established procedures for obtaining necessary electronic protected health information during an emergency. See Section 2.10, Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions, for more details.

Encryption, Decryption and Security via Facsimile

SBC Forensics has implemented a mechanism to encrypt and decrypt electronic protected health information whenever it is transmitting this information electronically. This mechanism utilizes a software program for encryption and authentication of transmitted data. SBC Forensics email systems will remain an encrypted format. Any transmission of protected health information will only be sent via TigerConnect HIPAA compliant application or securely with encrypted organizational email only.

Documentation and File Maintenance

SBC Forensics employees will have all documents related to each examination in a locked cabinet or drawer system that does not allow any person access to such files. If at any time files are not maintained in a locked and secure location it is grounds for immediate termination. Documentation and files are not allowed to remain in any vehicle at any time with exception of transporting required documents to court proceedings or other meetings that are required for law enforcement purposes. This includes camera or memory card devices used during patient forensic examinations.

Reporting and Investigating Security Breaches

Questions about breach of privacy issues will be presented initially to the Compliance Officer or SBC Forensics Administrative Team.

Employees who report possible security issues in good faith will not be subjected to retaliation or harassment as a result of the report. Concerns about possible retaliation or harassment will be reported to the primary physician of the practice.

Whenever a security issue has been identified, through monitoring, reporting of possible issues, investigations, or otherwise, the Compliance Officer shall have the responsibility and authority to take or direct appropriate action to address that issue. The corrective action will be set forth in writing

Corrective actions will be designed to ensure that the specific issues are addressed and similar problems do not occur in the future.

Employees who have engaged in willful misconduct will be subject to disciplinary action, up to and including termination in appropriate cases, in accordance with company policies, procedures and codes of conduct.

The results of inquiries will be made available to the primary physician. All employees are directed cooperate fully with any inquiries undertaken pursuant to this plan. To the extent

practical and appropriate, efforts will be made to maintain the confidentiality of such inquiries and the information gathered.

The Compliance Officer will maintain an incident log of security concerns that are reported, as described in this document. The log will record the issues, the individuals or departments affected, and the resolutions.

SBC Forensics and its employees are aware of the seriousness of security breaches and understand that appropriate action must be taken to prevent similar instances from occurring.

Organizational and Documentation Requirements

SBC Forensics has implemented the organizational and documentation requirements mandated by the HIPAA Security Rule. These requirements, and SBC Forensics's compliance declarations, are described in more detail in the following sections.

Documentation Form, Retention, Availability and Updates

SBC Forensics maintains these policies and procedures implemented to comply with the HIPAA Security Rule in written and electronic form. SBC Forensics retains the documentation required by HIPAA Security Rule for seven years from the date of its creation or the date when it last was in effect, whichever is later. SBC Forensics makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains. SBC Forensics reviews documentation periodically, and updates it as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Est: 4/5/2026

Policy and Procedure Manual

Subpoena Delivery and Confirmation

- Policy:* To establish procedures for the receipt, handling, delivery, and confirmation of subpoenas involving SBC Forensics personnel.
- Purpose:* To ensure employees understand proper subpoena procedures, protect employee privacy and safety, maintain accurate records, and support timely legal compliance.
- Procedure:* Personnel shall not provide personal home addresses or other personal location information to prosecutors, defense attorneys, law enforcement, private investigators, or other outside parties for subpoena service or legal correspondence.

Employees should utilize the organization's designated business contact information for matters related to employment duties whenever appropriate.

Receipt of a Subpoena by an Employee

If an employee personally receives a subpoena, notice to appear, legal request, or related court document connected to their role or duties, the employee must notify the Administrative Team immediately or as soon as reasonably possible.

A copy of the document must be provided through an approved secure method for recordkeeping and review.

Receipt of a Subpoena by the Organization

If SBC Forensics receives a subpoena or legal notice intended for an employee, the Administrative Team may forward the document to the employee using approved communication methods.

Employees may be required to acknowledge receipt promptly.

The organization may maintain records of delivery attempts, confirmations, acknowledgements, and related communications.

Designated Service Information

When appropriate, employees should provide the organization's approved business address, fax number, or other designated service contact information for employment-related legal notices.

Use of official organizational contact information helps protect employee privacy and supports proper document handling.

Compliance With Law

All subpoenas and legal service matters must comply with applicable federal, state, and local laws, court rules, and service requirements.

Nothing in this policy prevents lawful service where otherwise required.

Employee Responsibilities

Employees are expected to:

- Promptly notify leadership of legal notices related to work duties
- Cooperate with internal scheduling and response efforts
- Preserve related records or communications as instructed
- Maintain confidentiality regarding pending matters when appropriate

Administrative Authority

The Administrative Team reserves the right to determine appropriate internal handling, routing, verification, documentation, and communication procedures regarding subpoenas or legal notices.

Subpoena Delivery Address:
Forensic Examiner Name
c/o Butler County Sheriff's Office
5021 Winners Circle
West Chester, Ohio 45011

Facsimile Number:
1-866-444-7263

Est: 4/5/2026

Policy and Procedure Manual

Vehicle/Driving Safety

Policy: To establish safe driving expectations for all personnel operating company-owned or personal vehicles for SBC Forensics business purposes.

Purpose: To promote a culture of roadway safety, reduce accidents and injuries, protect employees and the public, and minimize organizational liability associated with business-related travel.

Procedure: All personnel who drive as part of their job duties are expected to operate vehicles safely, responsibly, and in compliance with all applicable laws.

This policy applies to:

- Company-owned vehicles
- Rental vehicles used for business purposes
- Personal vehicles used for work-related travel
- Travel between facilities, assignments, meetings, trainings, or other authorized work duties

Standards of Conduct

While operating a vehicle for business purposes, personnel must:

- Comply with traffic laws and licensing requirements
- Drive safely and defensively
- Use sound judgment and maintain professional conduct
- Operate vehicles in a manner that protects themselves, passengers, patients, and the public
- Avoid unnecessary risk-taking or careless behavior

The following conduct may result in disciplinary action up to and including termination:

- Driving under the influence of alcohol, illegal drugs, or impairing substances
- Unsafe use of prescription or over-the-counter medication while driving
- Reckless, aggressive, careless, or dangerous driving
- Driving without a valid license or with a suspended/restricted license
- Leaving the scene of an accident unlawfully
- Repeated moving violations or excessive points on driving record
- Distracted driving, including prohibited mobile device use
- Falsification of driving-related information
- Any conduct creating unacceptable safety or liability risk

Employee Responsibilities

Personnel who drive for work purposes must:

- Maintain a valid driver's license appropriate for the vehicle operated
- Maintain legally required auto insurance when using a personal vehicle
- Immediately notify the Administrative Team of license suspension, restrictions, lapse of insurance, or significant driving issues
- Wear seat belts as required by law
- Obey speed limits and adjust driving to road, weather, and traffic conditions
- Avoid texting, handheld phone use, or other distractions while driving
- Inspect vehicles for obvious safety concerns before use when practical
- Report accidents, damage, citations, near misses, or safety concerns promptly
- Keep vehicles reasonably clean, safe, and roadworthy when assigned responsibility
- Use professional judgment when traveling in hazardous weather or unsafe conditions

Fatigue and Safe Travel Expectations

Employees are expected to manage travel safely and avoid driving while fatigued.

Personnel should:

- Take appropriate rest breaks during longer trips
- Stop driving if too tired to continue safely
- Plan travel time realistically
- Notify leadership when schedules create safety concerns
- Seek lodging or alternative arrangements when extended travel creates unreasonable fatigue or risk

Use of Personal Vehicles

When using a personal vehicle for work-related duties:

- Prior authorization may be required
- Vehicle must be legally registered and insured
- Vehicle must be safe and suitable for intended travel
- Employees may be required to provide proof of insurance, registration, or license upon request
- Mileage reimbursement, if applicable, will follow current organizational policy

Accidents and Incidents

Any accident, collision, property damage, injury, citation, or significant near miss occurring during business travel must be reported to the Administrative Team as soon as reasonably possible.

Employees may be required to complete incident documentation and cooperate with internal or insurance reviews.

Driving Record Review

SBC Forensics may review employee driving eligibility, licensing status, insurance compliance, or motor vehicle records at hire, periodically, or at any time during employment.

If driving history or conduct presents unacceptable risk, the organization may impose restrictions, require corrective action, remove driving duties, or end employment/contract status.

Employer Responsibilities

SBC Forensics will seek to support safe driving practices by:

- Encouraging reasonable scheduling and travel expectations
- Discouraging unsafe driving behaviors
- Maintaining company vehicles when applicable
- Reviewing reported incidents and risks
- Taking corrective action when needed

Administrative Authority

The Administrative Team reserves the right to interpret this policy, determine driving eligibility, assess risk, modify travel expectations, and impose corrective action based on safety, insurance, operational, or liability concerns.

Policy and Procedure Manual

Drug Free Workplace Policy

Policy: To ensure SBC Forensics remains a drug free workplace for the safety of patients and personnel within the organization.

I. Statement of policy

Our company believes it's important to provide a safe workplace for all employees. This includes dealing with drug and alcohol use that negatively affects every workplace. Our company is concerned with the health and well being of all employees. Behaviors related to substance use can endanger all employees, not just the substance users. Our company cannot condone and will not tolerate:

- Possession of illegal drugs on company property and in an employee's system on the job;
- Possession of alcohol on company property and/or in an employee's system on the job;
- Sale, purchase, transfer, trafficking, use or possession of any illegal drugs on the job;
- Arrival or return to work with illegal drugs or alcohol in an employee's system to the extent that job performance or safety is affected.

We exempt physician prescribed medications to an employee who takes the medicine as prescribed and does not compromise workplace safety.

SBC Forensics is committed to this drug-free policy (Policy). It establishes clear guidelines for acceptable and unacceptable employee behavior in the workplace. We will not tolerate substance use in violation of this Policy. We intend to hold everyone reasonably responsible for supporting the Policy.

This Policy describes our company's drug-free workplace program. We expect every employee to read and understand it. The Policy applies to every employee. This includes top management and contractors. Anyone who violates this Policy will be subject to the consequences stated in this document.

We intend to hold all employees accountable in terms of substance use. However, we will support employees who voluntarily identify their substance problems prior to testing.

Regardless, we will subject employees, who have substance problems but do not come forward and then test positive for drug or alcohol use, to the employment consequences stated in the policy.

This Policy and program will go into effect within 60 days of the announcement of our drug-free program and the sharing of this Policy. The program's five key parts are:

- The written policy, which clearly spells out the program rules and how everyone benefits;
- Annual substance awareness education for employees;

- Annual training for supervisors regarding their responsibilities;
- Drug and alcohol testing, the most effective way to change harmful behaviors related to substance use;
- Employee assistance.

Employees will have the opportunity to learn about how substance use affects the workplace, and the signs and symptoms of substance abuse. Employees also can learn about the dangers of substance use, and how and where to get help for themselves and their families.

The SBC Forensics Administrative Team will be our drug-free coordinator. So, everyone knows who to go to for information or help. The SBC Forensics Administrative Team will arrange drug and alcohol testing, as needed. The SBC Forensics Administrative Team also can share where employees can go to for help for themselves and their families if they have a substance problem. He or she will also arrange to get knowledgeable presenters to educate everyone about substance use.

Protections for employees

Our program protects employees from dangerous and unproductive behaviors attributable to substance use. It also has built-in protections of employee rights.

- We keep employee records, such as testing results and referrals for help, confidential. We share information on a need-to-know basis only. Violation of confidentiality rights is subject to disciplinary action up to and including termination of employment.
- We're committed to employees who have a substance problem getting help. We will review each situation. Employee assistance is available for employees and their families through a list of resources available through our drug-free coordinator. We want you to come forward if you have a problem. Remember, if you test positive, you risk losing your job, and we don't want that to happen.
- We will train supervisors in their duties related to testing before this program begins. They will also receive annual training to identify behaviors that may indicate a substance problem exists. Supervisors will learn how to refer employees for assistance and/or testing.
- Random testing deters drug use in violation of the Policy. It also ensures we maintain confidence in our employees' abilities to perform their duties. We contracted with an outside vendor to handle random testing pools and select employees for drug testing at any time each year.
- We will provide employee identification numbers for use in the random drawings. The contractor will, in turn, furnish us with a list of individuals to test at the beginning of each selection period. It's our responsibility to notify each employee of his or her selection. We will also notify each employee of the date, time and location of the random testing.
- When notified, it's the employee's responsibility to provide a urine specimen for drug testing. An employee's failure to comply with the request for a specimen for random testing will result in consequences. This may include termination of employment.

Substances to be tested for and methods of testing

- Systems presence testing is the procedure used. This is how qualified testing professionals identify the presence of one or more of prohibited controlled substances or alcohol that may be present in the employee.
- If the initial screening test proves negative, then a negative test is declared. The qualified testing professional does a second test, called a confirmatory test, only if the initial test is non-

negative. This means the results came in at or higher than the cut-off level for one or more drugs. There is also a confirmatory test for alcohol when the preliminary test is at or above the specified cut-off level.

- Experts and the courts consider the confirmatory test 100 percent accurate. Scientific experts identified standard cut-off levels for each of the tested drugs after years of research. And employers have used these successfully for decades for both federal testing and non-regulated workplace testing (your drug-free program). Professionals use these levels to interpret all drug screens/tests, including the drugs for which testing may occur under our drug-free Policy. We reserve the right to add or delete substances on the list above, especially if mandated by changes in existing federal, state or local regulations or laws.
- For alcohol testing, a medical clinic that uses only certified equipment and personnel will conduct testing. We will consider breath alcohol concentrations exceeding [fill in the cut-off level your company has chosen with advice from legal counsel, such as .04] a verified positive result. In the event of an accident where an employee has blood alcohol drawn at a medical treatment facility, we will consider a result equal to or greater than [fill in cut-off level]
- a verified positive result. The collection site will typically use an Evidentiary Breath Test (EBT) to confirm any initial positive test result performed through saliva or breath testing.
- We will terminate employees adulterating, attempting to adulterate or substituting a specimen or otherwise manipulating the testing process. We will consider refusal to produce/provide a specimen a positive test unless there's a verifiable medical reason.

Specimen collection procedure

- Trained collection personnel who meet standards for urine collection and breath alcohol testing will conduct testing. We require confidentiality from our collection sites and labs.
- We permit employees to provide urine specimens in private, but subject to strict scrutiny by collection personnel. This avoids any alteration or substitution of the specimen.
- Likewise, the collection site will conduct breath alcohol testing in an area that affords the individual privacy. In all cases, there will only be one individual tested at a time.
- We will consider failure to appear for testing when scheduled refusal to participate in testing. Such failure will subject an employee to the range of disciplinary actions, including dismissal, and an applicant to the cancellation of an offer of employment. An observed voiding will only occur if there is grounds for suspecting manipulation of the testing process.
- Everyone will attend annual education sessions. Sessions will include sharing assistance resources.
- A local clinic identified by the SBC Forensics Administrative Team will collect urine specimens and conduct breath testing. A laboratory certified by the federal government will analyze urine specimens for drugs. These labs ensure various substances present in an employee are of sufficient quantity to be a danger in the workplace. This system ensures the accuracy and fairness of every test. We also have a medical review officer (MRO), a physician trained in substance abuse, involved. When the MRO receives positive test results, he or she contacts the employee and any appropriate health-care provider or pharmacy. The MRO then can determine whether there is a valid reason for the presence of the drug in the person's system.
- Our testing program starts with an initial screening test. If the initial results are positive, the laboratory then uses a second test or confirmatory test. We established cut-off levels for each drug and for alcohol to determine what we will consider a positive test. These levels show the employee didn't just have a little of the substance in his or her system but enough to affect workplace safety and the ability to do the job. These cut-off levels come from federal guidelines and are fair for all employees.

Employee education

Every employee will attend a session in which we discuss this Policy. You will have a chance to ask questions. We will distribute written copies of the Policy. We expect everyone to sign it; thus, confirming they received a copy. Later, we'll have a qualified person explain why substance use is a workplace problem. He or she will also explain the effects of various substances, signs/symptoms of substance use, and effects of commonly used drugs in the workplace and how to get help. Education aimed at getting everyone to understand the dangers of substance use will occur each year.

Supervisor training

We will train supervisors to recognize substance problems that may endanger the employee and others. They will also learn how to recognize Policy violations. Once trained, they will recognize behaviors that may demonstrate an alcohol/ drug problem, how to make referrals for help and for testing.

Drug and alcohol testing

We will test for drugs and for alcohol to detect problems and get employees not to use substances in a way that violates our Policy. Testing will also allow us to take appropriate action to correct the situation.

Employee assistance

Our company believes in offering assistance to employees with a substance problem. We will offer the following help. SBC Forensics will make available to employees a list of local community resources to turn to for help. This list includes places to go for an assessment and for treatment.

II. When may testing occur?

We will test employees for the presence of drugs in the urine and/or alcohol (through saliva, breath and/or blood) under any of the conditions outlined below.

A. Post-offer, pre-employment, and/or new hire drug testing , randomly

All applicants must undergo a drug test. A contractor whom we designate prior to employment will collect a urine specimen and a federally-certified laboratory will conduct the test. Any offer of employment depends upon satisfactory completion of this examination and/or screening. We and our examining physician will then determine if the applicant can perform the responsibilities of the position. New employees must submit to drug testing within 21 days of hire.

B. Reasonable suspicion testing

We will conduct reasonable suspicion testing when a supervisor suspects an employee may be in violation of this Policy. Management will document the suspicion in writing prior to the release of the test findings. A reasonable suspicion test may occur based on:

- Observed behavior, such as direct observation of drug/alcohol use or possession and/or physical symptoms of drug and/or alcohol use;
- A pattern of abnormal conduct or erratic behavior;
- Arrest or conviction for a drug-related offense or identification of an employee as the focus of a criminal investigation into illegal drug possession, use or trafficking. The employee must notify the company within five working days of any drug-related conviction;
- Information provided either by reliable and credible sources or independently corroborated regarding an employee's substance use;
- Newly discovered evidence the employee tampered with a previous drug or alcohol test;
- Reasonable suspicion testing does not require certainty. Mere hunches, however, do not justify testing. To prevent this, we will train all managers/supervisors to recognize drug and alcohol-related signs and symptoms. Testing may be for drugs or alcohol, or both.

C. Post-accident testing

We will conduct post-accident testing whenever an accident occurs. We consider an accident an unplanned, unexpected or unintended event that occurs on our property during the conduct of our business or during working hours, or which involves one of our motor vehicles or a personal motor vehicle used in conducting company business, or is within the scope of employment and which results in any of the following:

- A fatality of anyone involved in the accident;
- Bodily injury to the employee and/or another person that requires off-site medical attention away from the company's place of employment;
- Vehicular damage
- Non-vehicular damage

When such an accident results in one of the situations above, we will test any employee who may have caused or contributed to the accident for drugs or alcohol use, or both.

Drug and/or alcohol testing after an accident

Once we determine a need to test, urine specimen collection and/or breath/saliva or blood (for alcohol) must occur as soon as possible after we determine a need to test. We will consider any employee who seeks to delay providing a specimen as refusing to be tested.

Employees responsible for a work-related accident in which he or she was injured must grant us the right to request attending medical personnel obtain appropriate specimens. These include breath, saliva and/or blood to conduct alcohol testing and urine to conduct drug testing.

Employees grant us access to any and all other medical information that may be relevant in conducting a complete and thorough investigation of the work-related accident. This includes a full medical report from the examining physician(s) or other health-care providers. As a

condition of employment, we require a signed consent-to-test form. We reserve the right to determine who may have caused or contributed to a work-related accident. We may also choose not to test after minor accidents if there is no violation of a safety or work rule, minor damage and/or injuries and no reasonable suspicion.

D. Follow-up testing after return to duty from assessment or treatment

We conduct this test of employees who previously tested positive but whose employment we did not terminate.

We require a negative return-to-duty test before we allow the employee to return to work. If the employee fails this test, this will result in termination of employment. Once an employee tests negative and returns to duty, management will ensure additional tests occur. Any employee with a second positive test result will be termination of employment. Follow-up tests will be unannounced. They may occur at any time for a time period management considers reasonable. The intent is to deter any subsequent use that would violate the company's Policy and result in termination of employment.

E. Random drug testing

We conduct random drug testing of all employees on an unannounced basis. Computer software, used by an outside vendor, ensures that random, neutral selection occurs. We include all employees in each random draw. Each

V. Review of test results

To ensure we treat every tested employee fairly, the collection site uses the services of an MRO. The MRO is a doctor with a specialized knowledge of substance abuse disorders. He or she can determine whether there are any valid reasons for the presence in the employee's system of the substance that was tested positive. We follow the federal requirement that the MRO may not be affiliated with the federally-certified lab that does the urine analysis. SBC Forensics will identify the MRO used.

VI. Employees' rights when there's a positive test result

Upon receipt of a confirmed positive finding, the MRO will attempt to contact the employee by telephone or in person. If the MRO makes contact, he or she will inform the employee of the positive finding. The MRO will give the employee an opportunity to rebut or explain the findings.

The MRO can request information on recent medical history. He or she can also ask for medications taken within the last 30 days by the employee. If the MRO finds support in the employee's explanation, he or she may ask the employee to provide documentary evidence to support his or her position. Evidence can include treating physicians and pharmacies, which filled prescriptions, etc.

A failure on the part of the employee to provide documentary evidence will result in the MRO issuing a positive report with no attendant medical explanation. A medical disqualification of the employee will result. If the employee fails to contact the MRO as instructed, the MRO will issue a report of a positive test result.

VII. Reporting of results

The collection facility will report all test results to the MRO prior to reporting the results to us. The MRO will receive a detailed report of the findings of the analysis from the testing laboratory. The collection facility will list each substance tested along with the results of the testing.

We will receive a summary report, which indicate the employee passed or failed the test. We intend these procedures to be consistent with guidelines for MROs, published by the Department of Health and Human Services.

VIII. Storage of test results and right to review test

We will store all records of drug/alcohol separately from the employee's general personnel documents. We will maintain these records under lock and key. We limit access to designated company officials.

We will use the information only to properly administer this Policy and to provide to certifying agencies for review as required by law. We charge designated company officials with access to records with the responsibility for maintaining their confidentiality. Any breach of confidentiality may be an offense resulting in termination of employment.

Any employees tested under this Policy have the right to review and/or receive a copy of their own test results. An employee may request to receive his or her test results by giving the drug-free coordinator a duly notarized Employee Request for Release of Drug Tests Results form. We will use our best efforts to promptly comply with this request. And we will issue to the employee a copy of the results personally or by U.S. Certified Mail, Return Receipt Requested.

IX. Positive test results

We will immediately take employees found to have a confirmed positive drug or alcohol test off safety-sensitive duties. We will subject these employees to discipline up to and including termination.

X. Termination notices

In those cases where substance testing results in the termination of employment, termination notices will list misconduct as the reason. We will deem termination for cause.

Policy and Procedure Manual

Mobile Device Policy

Policy: To establish standards for the appropriate, secure, and professional use of mobile devices by SBC Forensics personnel.

Purpose: To protect confidential information, maintain cybersecurity, support productivity, and ensure that mobile devices used for work purposes do not create privacy, safety, or operational risks.

Scope: This policy applies to all personnel who:

- Use a personal device for work purposes
- Use a company-owned device
- Access company systems, applications, email, or data from any device
- Bring a mobile device onto company property or partner facilities while working

Mobile devices include, but are not limited to:

- Smartphones
- Cell phones
- Tablets
- Laptops
- Wearables
- Portable electronic devices

Use of Personal Devices for Work

Use of a personal device for work purposes may require prior approval by management.

Employees using personal devices for business purposes may be required to install company-approved **Mobile Device Management (MDM)**, security, or access-control software.

Failure to comply with required security controls may result in denial or removal of access to company systems or data.

Company-Owned Devices

Company-issued mobile devices remain the property of SBC Forensics and are provided for business use.

Limited personal use may be permitted if it does not interfere with operations, create excess cost, or violate policy.

The organization reserves the right to monitor, manage, restrict, recover, or reassign company-owned devices at any time.

Acceptable Use

Employees are expected to use mobile devices responsibly and professionally.

Personnel must:

- Use devices in compliance with all company policies
- Protect confidential, patient, and business information
- Limit personal use during working time
- Silence devices during meetings, exams, or professional interactions when appropriate
- Use devices only for legitimate business purposes while connected to company systems

Excessive personal use that interferes with productivity or workplace operations may result in corrective action.

Security Requirements

Devices used to access company information must maintain reasonable security safeguards, which may include:

- Password, PIN, or biometric protection
- Automatic lock settings
- Current operating system and software updates
- Encryption where required
- Approved applications only
- Multi-factor authentication when available

The organization may prohibit access from devices that are unsupported, insecure, rooted, jailbroken, compromised, or otherwise noncompliant.

Data Protection

Employees may not:

- Store company or patient information in unauthorized applications
- Transfer work data to personal cloud storage or unapproved services
- Share passwords or security credentials
- Circumvent security controls
- Disable company-installed security software
- Download illegal, pirated, or unauthorized software on devices used for work

Company access may be limited based on role-based permissions.

Privacy and Monitoring

Employees should have no expectation of privacy regarding company data, systems, or communications conducted through organizational networks, accounts, or company-owned devices, subject to applicable law.

SBC Forensics reserves the right to monitor, review, preserve, restrict, or remove company-related data accessed through its systems or devices.

Devices used for company business may be subject to inspection or security review when necessary.

Camera, Recording, and Social Media Restrictions

Use of cameras, video, livestreaming, screenshots, or audio recording on mobile devices is prohibited in patient care areas, exam areas, workspaces, or any setting where confidential information may be exposed, unless specifically authorized.

Employees may not use devices to capture, store, or transmit confidential information.

Accessing social media during work hours may be restricted based on job duties, operational needs, or network security requirements.

Driving and Safety

Employees must comply with all laws regarding mobile device use while driving.

Use of handheld devices while driving for work purposes is prohibited unless safely parked or legally hands-free.

Employees working in hazardous or sensitive environments must avoid device use when it creates a safety risk.

Lost, Stolen, or Damaged Devices

Employees must immediately report any lost, stolen, hacked, compromised, or damaged device used for work purposes.

To protect company data, SBC Forensics may remotely disable access or remove company data from affected devices.

The organization is not responsible for loss of personal data resulting from security actions taken to protect company systems.

Separation of Employment

Upon resignation, termination, leave status, or role change, company access may be removed and company data may be deleted from personal or company-owned devices.

All company-owned devices must be returned promptly upon request.

Family / Third-Party Access

Employees are responsible for ensuring that family members or other unauthorized persons do not access devices used for company purposes.

Sharing passwords, stored biometrics, or access credentials that allow entry to company information is prohibited.

Violations

Violation of this policy may result in disciplinary action up to and including suspension, termination, legal action, or revocation of device/network access.

Administrative Authority

The Administrative Team reserves the right to interpret, modify, enforce, and administer this policy and determine appropriate device security standards, access permissions, and corrective actions.

Est: 4/5/2026

Policy and Procedure Manual

Code of Conduct Policy

Policy: SBC Forensics expects all employees, contractors, volunteers, and representatives to conduct themselves with honesty, professionalism, loyalty, integrity, and sound judgment at all times.

Personnel are expected to act in the best interests of the organization, protect confidential and proprietary information, maintain professional relationships, and avoid conduct that harms operations, reputation, patients, or business interests.

Purpose: To establish standards of professional behavior, ethical conduct, confidentiality, conflict management, and accountability for all personnel representing SBC Forensics.

Scope: This policy applies to all:

- Employees
- Contractors
- Temporary staff
- Volunteers
- Supervisors and leadership
- Anyone acting on behalf of SBC Forensics

This policy applies during working time, on-call duties, travel, trainings, meetings, electronic communications, and any situation where an individual is representing or connected to SBC Forensics.

General Standards of Conduct

All personnel are expected to:

- Act honestly and ethically
- Perform duties competently and responsibly
- Treat patients, coworkers, facilities, and partners with professionalism and respect
- Follow policies, procedures, protocols, and lawful directives
- Protect organizational assets and information
- Use sound judgment in decision-making
- Maintain appropriate professional boundaries
- Avoid conduct that creates unnecessary risk or liability
- Support a cooperative and respectful workplace

Confidentiality and Proprietary Information

Employees must protect confidential, sensitive, and proprietary information obtained through employment or service.

This includes, but is not limited to:

- Policies and procedures
- Training materials
- Business strategies
- Pricing, contracts, and vendor relationships
- Scheduling systems or staffing models
- Operational methods
- Clinical workflows
- Internal communications
- Financial information
- Trade secrets
- Patient or partner information

Personnel may not use, copy, disclose, remove, share, transmit, or exploit such information except for legitimate authorized business purposes.

Unauthorized disclosure may result in immediate disciplinary action.

Loyalty / Conflict of Interest

Employees are expected to avoid conflicts between personal interests and the interests of SBC Forensics.

Examples may include:

- Using company information to benefit another business or competitor
- Assisting another organization in developing competing services using insider knowledge
- Diverting business opportunities, contracts, referrals, or relationships
- Misusing company time, resources, contacts, or property for outside ventures
- Engaging in outside activities that interfere with duties or create divided loyalty

Potential conflicts of interest must be disclosed to the Administrative Team.

Personnel must place their professional obligations to SBC Forensics first while on duty, on call, or performing assigned responsibilities.

Examples of conflicts of interest may include, but are not limited to:

- Using company information, training, systems, or relationships to benefit another business, employer, or competitor
- Assisting another organization in developing competing forensic, consulting, staffing, or related services
- Diverting referrals, contracts, opportunities, patients, facilities, or business relationships away from SBC Forensics
- Accepting outside compensation that interferes with duties or creates divided loyalty

- Using company time, equipment, contacts, or resources for another employer or venture
- Supervising, scheduling, influencing, or making decisions involving a family member, romantic partner, or close associate without disclosure
- Financial interests in vendors, contractors, facilities, or businesses doing business with SBC Forensics without disclosure
- Outside employment that creates scheduling conflicts, fatigue concerns, performance issues, confidentiality risks, or competition concerns

Second Employment / Outside Work

Employees may hold outside employment only if it does not:

- Involve misuse of confidential or proprietary information
- Compete directly or indirectly with SBC Forensics
- Damage relationships with facilities, partners, or clients
- Create actual or perceived divided loyalty

Employees may be required to disclose secondary employment or outside business activity to the Administrative Team. SBC Forensics reserves the right to review outside employment and determine whether a conflict exists.

If leadership determines that outside employment creates a conflict, operational burden, confidentiality concern, or business risk, the employee may be required to resolve the conflict as a condition of continued employment.

Duty to Disclose

Employees must promptly disclose any actual, potential, or perceived conflict of interest to the Administrative Team.

Failure to disclose outside employment or other conflicts may result in disciplinary action up to and including termination.

Relationships with Outside Organizations

Personnel must maintain professional relationships with hospitals, facilities, agencies, vendors, and community partners.

Employees may not independently negotiate, promise services, disclose internal operations, or represent company positions to outside organizations without authorization.

Any attempt to use company relationships for personal gain or to benefit another entity is prohibited.

Use of Company Property and Resources

Personnel must use company property, systems, records, equipment, accounts, and resources responsibly.

Misuse includes, but is not limited to:

- Unauthorized access or sharing
- Personal business use beyond reasonable limits
- Theft or removal of property
- Destruction or sabotage
- Improper copying of materials or data

Honesty and Reporting Obligations

Employees are expected to be truthful and cooperative in all work matters.

Personnel must promptly report:

- Policy violations
- Theft or misuse of information
- Conflicts of interest
- Fraudulent activity
- Security concerns
- Unethical conduct
- Misconduct that may harm the organization

Failure to report known serious misconduct may itself violate this policy.

Professional Behavior

The following may violate this policy:

- Dishonesty or deception
- Insubordination
- Harassment or discrimination
- Retaliation
- Breach of confidentiality
- Unprofessional conduct
- Conduct damaging to morale or teamwork
- Behavior harming reputation or business relationships
- Conduct inconsistent with organizational values

This list is not exhaustive.

Investigations

SBC Forensics may investigate suspected misconduct, conflicts of interest, misuse of information, or other violations.

Employees are expected to cooperate fully and honestly in investigations.

Failure to cooperate may result in corrective action.

Corrective Action

Violations of this policy may result in disciplinary action up to and including:

- Coaching or counseling
- Written warning
- Suspension
- Removal from duties or access
- Termination
- Legal action
- Injunctive relief or recovery of damages where applicable

The organization may act immediately in cases involving confidentiality breaches, theft of proprietary information, dishonesty, or serious misconduct.

Non-Retaliation

Employees who report concerns in good faith or participate in investigations are protected from retaliation.

Retaliation may result in disciplinary action.

Administrative Authority

The Administrative Team reserves the right to interpret, administer, revise, and enforce this policy and determine whether conduct is inconsistent with organizational expectations or business interests.

Est: 4/5/2026

Policy and Procedure Manual

Workplace Violence Policy

Policy: SBC Forensics is committed to maintaining a safe, respectful, and professional workplace free from violence, threats, harassment, intimidation, and conduct that undermines operations, safety, confidentiality, or public trust.

This policy also establishes standards for employee use of social media, online platforms, and electronic communications.

Purpose: To protect employees, patients, partner agencies, facilities, and the organization from workplace violence, unsafe behavior, reputational harm, confidentiality breaches, and inappropriate online conduct.

Section 1: Workplace Violence Policy

Zero Tolerance Standard

SBC Forensics does not tolerate workplace violence or threatening behavior committed by or against employees, contractors, patients, visitors, vendors, or other parties.

Violence, threats, intimidation, harassment, or disruptive conduct may result in immediate corrective action.

Prohibited Conduct

Examples of prohibited behavior include, but are not limited to:

- Physical assault or attempted assault
- Threatening statements, gestures, or intimidation
- Aggressive, hostile, or abusive conduct
- Harassment creating fear or emotional distress
- Intentional damage to property
- Possession of unauthorized weapons while working or on company property
- Domestic violence impacting the workplace
- Stalking or repeated unwanted contact
- Conduct creating a safety risk to others
- Any behavior reasonably viewed as violent, threatening, or unsafe

Reporting Procedures

Any potentially dangerous, hostile, or threatening situation must be reported immediately to the Administrative Team or leadership.

Reports may be made confidentially to the extent practical. All reports may be reviewed and investigated as appropriate.

Retaliation against any person making a good-faith report or participating in an investigation is prohibited.

Emergency Situations

If there is an immediate threat to safety:

- Contact emergency services (911) when safe to do so
- Follow facility emergency procedures
- Prioritize personal safety and the safety of others
- Notify leadership as soon as possible

Employees should not attempt to physically confront or disarm dangerous individuals unless necessary for immediate protection.

Prevention Measures

SBC Forensics may use reasonable safety measures including:

- Background checks where permitted by law
- Workplace safety reviews
- Security planning
- Incident investigations
- Corrective action
- Training and education

Enforcement

Violations may result in disciplinary action up to and including:

- Removal from duty
- Suspension
- Termination
- Law enforcement notification
- Legal action where appropriate

Section 2: Social Media and Online Conduct Policy

Policy Standard

Employees are expected to use sound judgment and professionalism when using social media, online platforms, messaging services, blogs, podcasts, forums, or any public electronic communication.

Online activity must not interfere with operations, damage professional relationships, compromise confidentiality, or negatively impact the mission of SBC Forensics.

Prohibited Online Conduct

Employees may not post, share, stream, record, transmit, or discuss any content involving:

- Patients or patient information
- Examinations or forensic processes
- Evidence or investigations
- Partner facilities or agencies
- Law enforcement matters
- Internal operations or workplace disputes
- Coworkers, leadership, or confidential personnel matters
- Logos, uniforms, badges, identification items, or internal materials without approval
- Nonpublic information learned through employment
- Content that is threatening, violent, harassing, sexually explicit, discriminatory, or otherwise unprofessional
- Any material that may reasonably harm the reputation, efficiency, safety, or working relationships of the organization

This applies whether names are used or not and includes photos, screenshots, videos, livestreams, comments, coded references, or indirect descriptions.

Representation of the Organization

Employees may not present themselves as an authorized spokesperson or official representative of SBC Forensics without prior written approval.

Use of company titles, logos, branding, uniforms, badges, or corporate email addresses for personal online activity is prohibited unless specifically authorized.

Employees creating approved public communications must clearly follow organizational direction.

Use During Work Time

Use of social media or personal online platforms during working time may be restricted or prohibited, including during:

- Patient care
- Examinations
- Meetings
- Trainings
- Administrative duties
- While on the premises of partner facilities
- Any time it interferes with job responsibilities

Investigations and Compliance

Where permitted by law, the organization may review publicly available information or information relevant to an internal investigation involving employee conduct, confidentiality, workplace disruption, safety, or policy compliance.

Non-Retaliation

SBC Forensics prohibits retaliation against employees who report suspected violations or cooperate in investigations in good faith.

Administrative Authority

The Administrative Team reserves the right to interpret, administer, investigate, and enforce this policy and determine whether conduct is inconsistent with organizational standards.

Violations may result in disciplinary action up to and including termination.

Est: 4/5/2026

Policy and Procedure Manual

Sexual Harassment Policy

Policy: SBC Forensics is committed to maintaining a professional work environment free from sexual harassment, unlawful harassment, discrimination, retaliation, and inappropriate conduct.

Sexual harassment of employees, contractors, applicants, patients, vendors, visitors, or any other individuals associated with the organization will not be tolerated.

Purpose: To promote a respectful workplace, protect employees and others from harassment, establish reporting procedures, and ensure prompt review of concerns.

Scope: This policy applies to:

- Employees
- Contractors
- Volunteers
- Applicants
- Supervisors and leadership
- Vendors
- Patients
- Visitors
- Any person interacting with SBC Forensics personnel in a work-related setting

This policy applies in:

- Offices and workplaces
- Hospitals and partner facilities
- Training events and conferences
- Meetings
- Business travel
- Company vehicles
- Electronic communications
- Social media or online interactions connected to work

Definition of Sexual Harassment

Sexual harassment includes unwelcome sexual conduct, requests for sexual favors, sexual advances, or other verbal, nonverbal, visual, written, or physical conduct of a sexual nature when:

- Submission to the conduct is made explicitly or implicitly a condition of employment
- Submission to or rejection of the conduct is used as the basis for employment decisions

- The conduct interferes with work performance
- The conduct creates an intimidating, hostile, offensive, or abusive work environment

Sexual harassment may occur regardless of gender, sex, sexual orientation, gender identity, or position.

Examples of Prohibited Conduct

Examples include, but are not limited to:

- Unwanted sexual advances
- Requests for dates or sexual favors after refusal
- Inappropriate touching, blocking movement, or invading personal space
- Sexual jokes, comments, innuendo, or gestures
- Comments about a person's body, appearance, clothing, or sex life
- Sending sexual texts, messages, images, memes, or emails
- Repeated flirtation after being told to stop
- Displaying sexually suggestive materials in the workplace
- Threats or promises tied to romantic or sexual cooperation
- Stalking or repeated unwanted attention
- Retaliation after rejection or complaint

This list is not exhaustive.

Professional Expectations

All personnel are expected to:

- Treat others with dignity and respect
- Maintain professional boundaries
- Use sound judgment in all workplace interactions
- Avoid conduct that could reasonably be viewed as harassing or inappropriate
- Immediately stop behavior when told it is unwelcome

Supervisors and leadership are expected to model appropriate conduct and respond promptly to concerns.

Reporting Procedures

Any employee who experiences, witnesses, or becomes aware of possible sexual harassment should report it promptly to:

- The Administrative Team
- A supervisor or manager
- Ownership or executive leadership
- Any designated reporting contact

Employees are encouraged to report concerns even if they are unsure whether conduct violates this policy.

Reports may be verbal or written.

If the complaint involves someone in leadership, employees may report to another member of management or ownership.

Investigation Process

SBC Forensics will review complaints promptly and take action as appropriate.

The organization may:

- Interview involved parties or witnesses
- Review messages, documents, or other evidence
- Implement interim measures during review
- Maintain confidentiality to the extent practical

All employees are expected to cooperate honestly in investigations.

Non-Retaliation

Retaliation is strictly prohibited against anyone who:

- Reports a concern in good faith
- Participates in an investigation
- Provides information or witness statements
- Opposes conduct believed to violate this policy

Retaliation itself is a policy violation and may result in disciplinary action.

Corrective Action

If inappropriate conduct is substantiated, SBC Forensics may take corrective action up to and including:

- Coaching or counseling
- Written warning
- Training requirements
- Removal from assignments
- Suspension
- Termination
- Vendor removal or contract termination
- Reporting to licensing boards or law enforcement where appropriate

The organization may take action even if conduct does not rise to the level of unlawful harassment but violates professional standards.

False or Bad-Faith Complaints

Knowingly false accusations or intentionally misleading information may result in disciplinary action. However, unsubstantiated complaints made in good faith will not result in discipline.

Administrative Authority

The Administrative Team reserves the right to interpret, administer, revise, and enforce this policy and determine appropriate responses consistent with organizational standards and applicable law.

Est: 4/5/2026

Policy and Procedure Manual

Social Media Policy

Policy: To establish expectations for employee use of social media, online platforms, and electronic communications in a manner that protects SBC Forensics, its patients, employees, partner agencies, and professional reputation.

Purpose: To ensure social media and internet use do not interfere with operations, violate confidentiality, damage professional relationships, compromise investigations, or negatively impact the mission of SBC Forensics.

Scope: This policy applies to all employees, contractors, volunteers, and representatives of SBC Forensics.

It applies to use of:

- Social media platforms
- Blogs
- Podcasts
- Forums
- Video platforms
- Messaging applications
- Personal websites
- Professional networking sites
- Any public or semi-public electronic communication platform

Examples include, but are not limited to:

- Facebook
- Instagram
- X / Twitter
- TikTok
- LinkedIn
- YouTube
- Snapchat
- Reddit
- Discord
- Future or emerging platforms

Professional Expectations

Employees are expected to use sound judgment and professionalism in all online activity.

Online conduct must not:

- Harm the reputation or mission of SBC Forensics
- Damage working relationships with hospitals, law enforcement, advocates, courts, or community partners
- Interfere with employee performance or workplace operations
- Undermine public confidence in the organization

Prohibited Content and Conduct

Employees may not post, share, stream, record, discuss, or distribute content involving:

- Patients or patient information
- Protected health information
- Forensic examinations or exam processes
- Evidence or chain of custody matters
- Active or past investigations
- Internal workplace matters
- Coworkers, leadership, or confidential personnel issues
- Partner hospitals or facilities
- Law enforcement or multidisciplinary team matters
- Trade secrets or confidential business information
- Logos, uniforms, badges, credentials, or identifying agency materials without approval
- Photos, videos, screenshots, recordings, or documents related to work activities
- Any content that is threatening, harassing, discriminatory, violent, sexually explicit, intimidating, or otherwise unprofessional

This applies even if names are omitted or information is partially disguised.

Representation of the Organization

Employees may not represent themselves as speaking on behalf of SBC Forensics unless expressly authorized in writing by the Administrative Team.

Employees may not create, manage, edit, or publish official SBC Forensics social media accounts or public-facing content without authorization.

Use of job title, organizational affiliation, corporate email, logo, badge, or branding for personal online activity is prohibited unless approved.

Personal Accounts

Employees using personal accounts should make clear that personal opinions are their own and do not represent the views of SBC Forensics.

Nothing in this policy prohibits lawful personal expression protected by applicable law; however, employees remain responsible for conduct that violates confidentiality, professionalism, safety, or other company policies.

Use During Work Time

Employees may be restricted from using personal social media or non-business online platforms during work hours, including during:

- Examinations
- Patient care
- Meetings
- Trainings
- Administrative duties
- While on partner facility property
- Any time use interferes with job performance

Investigations and Compliance

Where permitted by law, SBC Forensics may review publicly available online content or content relevant to internal investigations involving:

- Policy violations
- Misconduct
- Safety concerns
- Confidentiality breaches
- Operational disruption
- Reputational harm

Employees are expected to cooperate with lawful internal investigations.

Reporting Concerns / Non-Retaliation

Employees are encouraged to report suspected violations of this policy.

SBC Forensics prohibits retaliation against any individual who makes a good-faith report or participates in an investigation.

Violations

Violations of this policy may result in disciplinary action up to and including:

- Coaching or warning
- Suspension
- Removal of access privileges
- Termination
- Legal action where appropriate

Administrative Authority

The Administrative Team reserves the right to interpret, enforce, revise, and administer this policy and determine whether conduct is inconsistent with organizational standards.

Est: 4/5/2026

Policy and Procedure Manual

OSHA/Workplace Safety Compliance Policy

Policy: SBC Forensics is committed to providing a safe and healthful work environment for all employees and to maintaining compliance with applicable standards of the Occupational Safety and Health Administration (OSHA), state workplace safety laws, and related regulatory requirements.

Safety is a shared responsibility of leadership and all personnel.

Purpose: To promote workplace safety, reduce occupational injuries and illnesses, establish employee expectations, and ensure compliance with applicable safety regulations.

Scope: This policy applies to all:

- Employees
- Contractors
- Temporary personnel
- Volunteers
- Supervisors and leadership
- Individuals performing work on behalf of SBC Forensics

This policy applies in offices, vehicles, hospitals, partner facilities, training sites, storage locations, and any location where work duties are performed.

General Safety Standards

SBC Forensics will make reasonable efforts to maintain safe working conditions and may implement safety procedures, training, equipment requirements, and corrective actions as needed.

Employees are expected to:

- Follow all safety rules, procedures, and posted instructions
- Use good judgment and safe work practices
- Maintain awareness of surroundings and hazards
- Perform duties in a manner that protects themselves and others
- Immediately report unsafe conditions, injuries, exposures, or incidents
- Participate in required safety training
- Use required personal protective equipment (PPE)

Hazard Communication

Where hazardous chemicals or regulated substances are present, SBC Forensics will maintain applicable hazard communication practices consistent with regulatory requirements.

This may include:

- Safety Data Sheets (SDS) access where applicable
- Proper labeling
- Safe storage
- Employee training
- Spill response procedures

Employees must not handle hazardous materials unless trained and authorized.

Bloodborne Pathogens / Exposure Control

Because work may involve contact with bodily fluids, evidence, or clinical environments, personnel must follow infection prevention and exposure-control practices.

Employees are expected to:

- Use universal/standard precautions
- Wear appropriate PPE
- Dispose of sharps and contaminated materials properly
- Report exposures immediately
- Participate in required post-exposure procedures

Where applicable, the organization may maintain an Exposure Control Plan.

Personal Protective Equipment (PPE)

Employees must use PPE as required by job duties, facility standards, or safety conditions.

Examples may include:

- Gloves
- Masks or respirators where required
- Eye protection
- Gowns
- Protective footwear
- Other role-specific equipment

Failure to use required PPE may result in corrective action.

Injury and Incident Reporting

All work-related injuries, illnesses, exposures, near misses, or unsafe conditions must be reported immediately or as soon as reasonably possible to the Administrative Team.

Employees may be required to complete incident documentation.

The organization may investigate incidents and implement corrective measures.

Emergency Preparedness

Employees are expected to follow emergency procedures for fires, severe weather, workplace violence, hazardous exposures, medical emergencies, or other urgent events.

When applicable:

- Call 911 or local emergency services
- Follow host facility emergency procedures
- Notify leadership as soon as practical
- Prioritize life safety

Training

Employees may be required to complete safety training based on role, assignment, or legal requirements, including but not limited to:

- OSHA awareness
- Bloodborne pathogens
- PPE use
- Infection control
- Hazard communication
- Workplace violence prevention
- Ergonomics or lifting safety
- Emergency response

Failure to complete required training may affect work eligibility.

Records and Compliance

SBC Forensics may maintain workplace safety records, logs, training documentation, incident reports, and other records as required or deemed appropriate.

Employees are expected to cooperate with safety audits, inspections, investigations, and corrective actions.

Non-Retaliation

Employees may report safety concerns, injuries, hazards, or regulatory issues in good faith without fear of retaliation.

Retaliation for good-faith safety reporting is prohibited.

Corrective Action

Violations of safety rules, failure to report hazards, unsafe conduct, misuse of PPE, or refusal to follow required safety procedures may result in disciplinary action up to and including termination.

Administrative Authority

The Administrative Team reserves the right to interpret, administer, revise, and enforce this policy and implement additional safety procedures based on operational needs, hazards, facility requirements, or changes in law/regulation.

Est: 4/5/2026

Policy and Procedure Manual

Bereavement Leave Policy

Policy: SBC Forensics recognizes that employees may need time away from work following the death of a family member or loved one and is committed to providing bereavement leave when appropriate.

Purpose: To provide eligible employees with time off to grieve, attend funeral or memorial services, manage personal matters, and support family needs following a loss.

Bereavement Leave

Eligible employees may receive up to **15 paid hours** of bereavement leave per qualifying event, subject to scheduling needs, payroll eligibility, and management approval.

Bereavement leave may be used for:

- Funeral or memorial attendance
- Travel related to services
- Immediate family support needs
- Personal grieving time
- Related arrangements following a death

Notification Requirements

Employees requesting bereavement leave should notify the Administrative Team or on-call administration as soon as reasonably possible.

The request should include:

- Expected dates or hours needed
- General scheduling impact, if known
- Any additional leave needs, if applicable

Documentation may be requested where appropriate.

Additional Leave

Additional paid or unpaid leave, schedule adjustments, or use of available PTO may be approved at the discretion of the Administrative Team based on individual circumstances and operational needs.

Administrative Discretion

SBC Forensics reserves the right to determine eligibility, approve scheduling, request reasonable documentation, and administer this policy consistent with business needs and applicable law.

Est: 4/5/2026

Policy and Procedure Manual

Extended Leave Policy

Policy: SBC Forensics recognizes that employees may need extended time away from work for medical reasons.

Purpose: To provide eligible employees with time off as able within the confines of continuing daily operations.

Eligibility

Salaried part time or full-time personnel who are employed over 12 months who have worked a minimum of 910 hours within the 12 months that are unable to work for a medical or extended leave beyond 7 days of assigned workdays/shifts. Extended leave is only eligible for approval once within every 12 months.

Position Protection

The employee's position will be held for an approved absence up to 4 weeks (thirty days) at discretion of administration if the employee's absence will not cause significant harm to operations due to the absence. Position protection for absences beyond 4 weeks are at sole discretion of the employer.

Documentation

Written requests are required to be provided along with medical certification from a healthcare provider for leave requests that clearly define medical limitations, expected timeframe of absence. All employees must provide medical provider with the job description, and the medical provider must confirm that the employee is able to return to work performing all required duties without limitations

Salary Disbursement

Salaried employees that are approved for a valid extended leave may receive payment of their base salary not to exceed 2 (two) pay periods (including the pay period leave is initiated in. Salary is only paid for approved leave/ absences with appropriate documentation and if leave is approved by administration.

Policy and Procedure Manual

SBC Property Kit Sign-in

Policy: Procedure to sign biological evidence into the temporary SBC Forensics holding area.

Purpose: SBC Forensics personnel will follow the following procedures to sign any biological samples into the SBC Forensics property holding area.

Administration Notification

SBC Personnel will contact administration via Tigerconnect immediately if the need arises for temporary holding of biological specimens in the SBC Forensics holding area. Access is only granted for this under approval of administration including one of the following: law enforcement liaison on call for the day, administrator on call for the day.

Administration will require the following information prior to approval of the temporary holding. The below information will be sent by Tigerconnect prior to administration granting access to house the kit in our holding area. This information will also be documented in Themis along with all information from the mandatory reporting policy.

- 1. Law enforcement agency jurisdiction***
- 2. Reason why SBC temporary holding is being requested***
- 3. Name of on duty Sgt, Lt, Commander they spoke with from the PD. This MUST be someone in charge and not a street officer or dispatcher and should have authority to speak on behalf of evidence handling***
- 4. Phone number, name, badge number of a contact to arrange kit pick up the following day***
- 5. Inform the person you spoke with that SBC Administration will be in contact with them within 24 hours to arrange kit delivery details***
- 6. ALL of the above information must be charted in your forensic medical record***

Documentation on Kit

If granted access for temporary holding access for biological samples the examiner must follow the below documentation carefully as this is a best practice caution procedure. The documentation steps must be followed carefully.

Chain of Custody Documentation

The chain of custody will be completed through the following steps when the item is at the SBC Administration office and prior to being placed in the gray biological sample storage bin.

1. *Evidence Secured By: place the name of examiner, signature of examiner, Hospital Name/SBC Forensics/City, date and time box sealed in the appropriate area*
2. *Evidence Released By: place the name of the examiner, signature of the examiner, Hospital Name/SBC Forensics/City, **date and time must match the below evidence received by. This time is assigned by Themis when completing the chain of custody***
3. *Evidence Received By: SBC Property in the name of receiving agency, SBC Property in the signature of the receiving agency, **date and time must match above evidence released by. This time is assigned by Themis when completing the chain of custody.***

Property Room Form

The SBC Forensics Property Room form will be completed online which is found on the employee gateway should be completed with every submission into the SBC property holding without exception. It is required to be completed every time.

Est: 4/15/26

Policy and Procedure Manual

Mandatory Reporting

Policy: SBC Forensics personnel will follow mandatory reporting in accordance with Ohio Revised Code 2921.22 for felony crimes

Purpose: To define procedures for performing required mandated reporting of felony crimes as a mandated reporter in the State of Ohio.

All personnel performing forensic examinations will complete mandatory reporting in every instance in accordance with the Ohio Revised Code 2921.22 if they are made aware that a felony crime has occurred.

ORC Statutes of Felony Crimes to be Reporting:

Rape/Sexual Assault, Strangulation: in accordance with 2907.02, rape is a felony crime in the State of Ohio. In accordance with Ohio Revised Code 2903.18 strangulation is a felony crime in the State of Ohio. During the forensic examination, completing deferral form, or any encounter for a request of service or any interaction the examiner is required to complete the mandatory reporting to the appropriate law enforcement agency where the event occurred.

Failure to Report

Failure to report a felony crime is a misdemeanor of the fourth degree in the State of Ohio which may include imprisonment/jail time and a fine in accordance with Ohio Revised Code 2921.22. Failure to report a felony crime is also subject

Procedures for Mandatory Reporting:

The examiner will complete the mandatory reporting to the appropriate law enforcement agency, children's protective service, adult protective service agency immediately by phone on a recorded line with the appropriate entity. In every instance the examiner will document the following in the chart without exception. Every interaction is expected to have the below information documented in every instance without exception of any kind. Failure to perform these actions are subject to disciplinary action.

- Name AND title (dispatch, detective, officer, etc) of the person you spoke with on phone
- Badge Number of the person you spoke with on the phone
- Date and Timestamp of the interaction
- Reason you spoke with the person (ex: mandatory reporting, kit location, etc)

