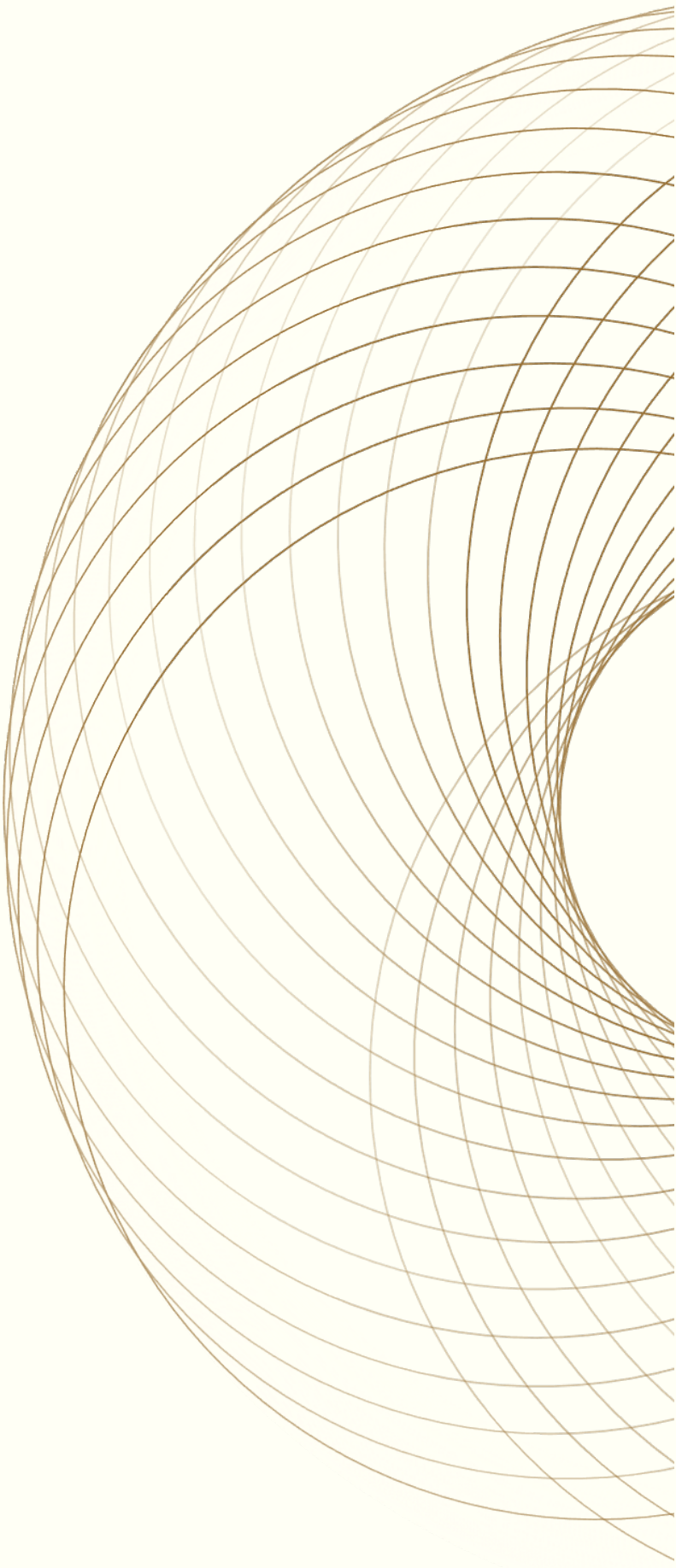
L I L A

# Contractor Handbook

## Lila Sciences



Last Updated

September 2026

# Table of Contents


PURPOSE OF CONTRACTOR HANDBOOK....1
COMMITMENT TO EQUAL EMPLOYMENT OPPORTUNITY....2
- Equal Employment Opportunity....2
- Sexual and Other Prohibited Harassment....2
- Accessibility and Site Access....6

SCREENING OF CONTRACTORS....6
- Background Screening....6

CONDUCT ON COMPANY PREMISES....6
- Speak-Up, Reporting, and Anti-Retaliation Policy....7
- Proprietary Information and Confidentiality....9
- Attire and Safety Requirements....10
- Social Media and Public Communications....10
- Contact with the Media....12
- Photography and Videography....12

WORKPLACE SAFETY AND SECURITY....13
- Anti-Violence Policy....13
- Anti-Bullying Policy....14
- Weapons in the Workplace....15
- Work-Related Injuries....18
- Smoke-Free Workplace....18
- Drug- and Alcohol-Free Workplace Policy....18
- Company's Right to Search....21
- Use of Company Equipment and Resources....21
- Business Equipment and Information Systems Usage Policy....22
- No Solicitation/Distribution of Literature....27
- Physical Security (BIZ-IT-SEC-015)....27

# PURPOSE OF CONTRACTOR HANDBOOK

This Contractor Handbook (the "Handbook") contains information about certain policies, procedures, and requirements applicable to independent contractors, consultants, service providers, and their personnel (collectively, "contractors") who perform services for Lila Sciences, Inc. (the "Company") on Company premises, at Company-sponsored locations, or through access to Company computer systems and networks. These policies are intended to promote workplace safety, security, legal compliance, protection of the Company's confidential and proprietary information, and efficient operation of the Company's facilities.

Contractors are expected to review this Handbook carefully and comply with its applicable requirements while providing services to the Company. This Handbook does not describe all Company policies and procedures that may apply to contractors, nor does it alter or replace the terms of any applicable service agreement, consulting agreement, statement of work, purchase order, or other contract governing the contractor's services.

This Handbook supersedes any previously issued contractor handbook or worksite rules communicated to you. The Company reserves the right to revise, amend, delete, or add to the provisions of this Handbook at any time. Any such revisions, amendments, deletions, or additions must be made in writing. No oral statements or representations may modify the provisions of this Handbook.

This Handbook is not a contract and does not create any contractual rights. Nothing in this Handbook creates an employment relationship between the Company and any independent contractor or contractor personnel. Contractors are engaged pursuant to the terms of their applicable contractual arrangements with the Company, and nothing in this Handbook shall be construed as creating an employer-employee relationship, altering a contractor's independent status, guaranteeing any duration of the contractor's engagement with the Company, or modifying any existing contractual relationship.

The policies contained in this Handbook are intended solely to address matters relating to workplace safety, security, legal compliance, workplace conduct, protection of Company personnel and property, confidentiality, and similar operational requirements. Nothing in this Handbook is intended to direct, control, or govern the manner or means by which contractors perform their services, which shall remain the sole responsibility of the contractor except as otherwise required by law or expressly set forth in an applicable contract.

Questions regarding this Handbook should be directed to the Company contact responsible for administering the contractor's engagement for the Company.

# COMMITMENT TO EQUAL EMPLOYMENT OPPORTUNITY

## Equal Employment Opportunity

The Company is an equal opportunity employer. In accordance with applicable law, we prohibit discrimination against any applicant or employee based on any legally Protected Characteristics, including, but not limited to: race, color, religion, sex, pregnancy (including lactation, childbirth or related medical conditions), sexual orientation, gender identity, age (40 and over), national origin or ancestry, citizenship or immigration status, physical or mental disability, genetic information (including testing and characteristics), veteran status (including status as a protected veteran), uniformed servicemember status or any other status protected by federal, state or local law (collectively, "Protected Characteristics"). Our commitment to equal opportunity employment applies to all persons involved in our operations, including contractors.

Any individual who believes that they or another individual has been subjected to discrimination in violation of this policy should report it pursuant to the *Complaint Procedures* in the *Sexual and Other Prohibited Harassment* policy below. If the Company determines this policy has been violated, appropriate action will be taken. For contractors, this may include restriction or revocation of facility access, removal from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

Retaliation is prohibited against any person by another employee or by the Company for reporting prohibited discrimination or for filing, testifying, assisting, or participating in any manner in any investigation, proceeding or hearing conducted by a governmental enforcement agency. An individual should report any retaliation prohibited by this policy pursuant to the *Complaint Procedures* in the *Sexual and Other Prohibited Harassment* policy below.

If a complaint of retaliation is substantiated, appropriate action will be taken. For contractors, this may include restriction or revocation of the contractor's facility access, removal from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

## Sexual and Other Prohibited Harassment

The Company is committed to providing a work environment that is free of harassment based on any legally Protected Characteristics. As a result, the Company maintains a strict policy prohibiting sexual harassment and harassment against any applicant or employee based on any legally-recognized status, including, but not limited to: race, color, religion, sex, pregnancy (including lactation, childbirth or related medical conditions), sexual orientation, gender identity, age (40 and over), national origin or ancestry, physical or mental disability, genetic information (including testing and characteristics), veteran status, citizenship or immigration status, uniformed servicemember status or any other status protected by federal, state or local law (collectively, "Protected Characteristics").

The harassment prohibited by this policy applies to conduct by any person involved in our operations. This policy specifically prohibits conduct that creates or contributes to a hostile or offensive working environment for any Company employee or applicant based on Protected Characteristics. If such harassment occurs that an individual believes to be a violation of this policy, the procedures set forth in the *Complaint Procedures* in this policy should be followed.

The Company prohibits unlawful harassment and sexual harassment and prohibits harassing conduct (as defined in this policy), even if such harassment does not rise to the level of being unlawful. This policy is not designed or intended to limit the Company's authority to take appropriate action for conduct that violates this policy that the Company deems unacceptable, regardless of whether that conduct satisfies the definition of unlawful harassment or sexual harassment.

***Sexual Harassment Defined***

Sexual harassment includes unwanted sexual advances, requests for sexual favors or visual, verbal, or physical conduct of a sexual nature when:

- Submission to such conduct is made a term or condition of employment; or
- Submission to, or rejection of, such conduct is used as a basis for employment decisions affecting the individual; or
- Such conduct has the purpose or effect of unreasonably interfering with an employee's work performance or creating an intimidating, hostile or offensive working environment, even if the individual making the report is not the intended target of such conduct.

Sexual harassment includes various forms of offensive behavior based on sex. The following is a non-exhaustive list of the types of conduct prohibited by this policy:

- Unwanted sexual advances or propositions (including repeated and unwelcome requests for dates);
- Offers of employment benefits in exchange for sexual favors;
- Making or threatening reprisals after a negative response to sexual advances;
- Visual conduct: leering, making sexual gestures, displaying sexually suggestive objects or pictures, cartoons, posters, websites, emails, or text messages;
- Verbal conduct: making or using sexually derogatory comments, innuendos, epithets, slurs, sexually explicit jokes, or comments about an individual's body or dress, whistling or making suggestive or insulting sounds;
- Verbal and/or written content of a sexual nature, graphic verbal and/or written sexually degrading commentary about an individual's body or dress or sexual

experiences, sexually suggestive or obscene letters, notes, invitations, emails, text messages, or other social media postings;

- Physical conduct: unwelcome or inappropriate touching, physical violence, intimidation, touching, assault or impeding or blocking normal movements;

- Hostile actions taken against an individual because of that individual's sex, sexual orientation, gender identity, or the status of being transgender, such as:

    - Interfering with, destroying, or damaging a person's workstation, tools, or equipment, or otherwise interfering with the individual's ability to perform the job;

    - Repeated and intentional use of a name or pronoun inconsistent with an individual's known gender identity;

    - Asking intrusive questions about a person's sexual orientation, gender identity, gender transition, or intimate body parts;

    - Sabotaging an individual's work; and

    - Bullying, yelling, or name-calling.

- Retaliation for making reports or threatening to report sexual harassment.

Sexual harassment can occur regardless of the gender of the person committing it or the person who is exposed to it. Harassment on the basis of sexual orientation, self-identified gender, perceived gender, or transgender status are all forms of prohibited sexual harassment.

***Other Types of Prohibited Harassment***

Harassment on the basis of any Protected Characteristic is prohibited. Prohibited harassment may include behavior similar to the illustrations above and may also include, but is not limited to:

- Verbal conduct including taunting, jokes, threats, epithets, derogatory comments, or slurs based on an individual's Protected Characteristics;

- Visual and/or written conduct including derogatory posters, photographs, calendars, cartoons, drawings, websites, social media, emails, text messages, or gestures based on an individual's Protected Characteristics;

- Sharing or watching pornography or sexually demeaning depictions of people, including AI-generated and deepfake images and videos;

- Mimicking or mocking a person's disability, accent, or religious garments, jewelry, or displays; and

- Physical conduct including assault, unwanted touching or blocking normal movement because of an individual's Protected Characteristics.

***Protection Against Retaliation***

The Company prohibits retaliation for using the complaint procedures provided below, reporting prohibited discrimination, harassment, sexual harassment or retaliation, objecting to such conduct or filing, testifying, assisting, or participating in any manner in any investigation, proceeding or hearing conducted by a governmental enforcement agency.

Individuals who believe they have been subjected to retaliation or believe that another individual has been subjected to retaliation, should report this concern pursuant to the *Complaint Procedure* in this policy. Any report of retaliatory conduct will be investigated in a thorough and objective manner.

If a report of retaliation prohibited by this policy is substantiated, appropriate action will be taken. For contractors, this may include restriction or revocation of the contractor's facility access, removal from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

***Complaint Procedures***

A contractor who believes that they or another individual has been subjected to discrimination, sexual harassment, any other form of prohibited harassment or retaliation should, as soon as possible, report it to the Company contact responsible for administering the contractor's engagement for the Company or using the Human Resources Inbox (HR@lila.ai).

***Investigation***

After a report is received, or the Company otherwise has reason to believe discrimination, prohibited discrimination, harassment, including sexual harassment, or retaliation is occurring, a timely, thorough, and objective investigation by the Company will be undertaken. The Company will maintain confidentiality surrounding the investigation to the extent possible, consistent with a thorough and objective investigation, and to the extent permitted or required under applicable law.

Once the investigation is completed and a determination is made, the complaining party will be advised that the investigation has been completed and may be informed of the resolution. The Company complies with the law in conducting investigations and expects that employees will cooperate with an investigation, except when voluntary compliance with an investigation is requested. Contractors are expected to provide truthful information when participating in an investigation.

***Remedial Action***

If the Company determines that this policy has been violated, prompt remedial action will be taken. For contractors, appropriate action may include restriction or revocation of facility access, removal from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

### Accessibility and Site Access

The Company is committed to providing safe and accessible facilities. Contractors who require reasonable modifications or assistance to access Company premises, participate in site-specific safety or evacuation procedures, or otherwise access Company facilities in connection with their engagement should contact the Company contact responsible for administering the contractor's engagement for the Company. Requests will be evaluated in accordance with applicable law and the Company's operational and safety requirements.

Nothing in this policy creates an employment relationship or entitles any contractor to employee benefits, privileges, or employment-related accommodations.

## SCREENING OF CONTRACTORS

### Background Screening

Consistent with applicable law and contractual requirements, the Company may require contractors and contractor personnel who access Company facilities, computer systems and networks, confidential and proprietary information, or other sensitive resources to satisfy background screening requirements established for the applicable engagement.

Contractors are responsible for ensuring that any personnel assigned to perform services for the Company satisfy applicable screening requirements, unless otherwise agreed in writing.

The Company reserves the right to deny, restrict, or revoke facility, system, or information access where screening requirements are not met or where permitted by law and consistent with legitimate business, safety, security, or compliance interests.

Any background screening will be conducted in accordance with applicable law and any contractual arrangements governing the contractor's engagement.

## CONDUCT ON COMPANY PREMISES

The Company expects contractors and contractor personnel performing services on Company premises to conduct themselves in a professional manner and to comply with applicable laws, rules, and regulations; contractual obligations in the contract governing the contractor's engagement; and Company policies and procedures relating to safety, security, workplace conduct, protection of Company property and the Company's confidential and proprietary information, and legal compliance.

#### *Prohibited Behavior and Expectations*

It is not possible to list all the forms of prohibited behavior at Company worksites, but below are examples of unacceptable behavior that may lead to restriction or revocation of a contractor's facility access, removal of a contractor from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion. The following list is not all-inclusive:

- Falsification of credentials, certifications, security information, invoices, reports, or business records of the Company;

- Theft or the deliberate or careless damage of the Company's property or the property of any person involved in the Company's business operations;

- Use or removal of materials, supplies, tools or products of the Company, a visitor or third-party involved in the Company's business operations without advanced permission from management;

- Provoking a physical fight or engaging in physical fighting while performing services for the Company or on premises owned or occupied by the Company;

- Carrying firearms, weapons, or dangerous substances at any time, on premises owned or occupied by the Company, unless otherwise permitted by applicable law.

- Using abusive, violent, threatening, or vulgar language while performing services for the Company or while on premises owned or occupied by the Company;

- Violating any policy, rule, or procedure of the Company as set forth in this Handbook;

- Use, consumption or possession of intoxicating beverages or illegal drugs while performing services for the Company or while on the Company premises.

- Discrimination or harassment in violation of our EEO or Sexual and Other Prohibited Harassment Policy against any employee, client, contractor, visitor, or other individual involved in the operations of the Company based upon race, religion, age, sex, national origin, disability, or any other protected characteristic under applicable law.

## Speak-Up, Reporting, and Anti-Retaliation Policy

### *We Encourage a Speak Up Culture*

Choosing to speak up about work-related concerns helps build a healthy, ethical, and compliant Company. The Company encourages individuals to speak up and raise questions and concerns promptly about any situation that may violate our policies or procedures; the laws, rules, and regulations that govern our business operations; and best practices in accounting, auditing, and financial reporting matters (collectively these are referred to in this policy as our "Code").

### *Raise Good Faith Questions and Concerns About Conduct that May Violate Our Code*

Consistent with our commitment to ethics and legal compliance, we welcome your good faith questions and concerns about any conduct that you believe may violate our Code.

We promote an environment that fosters good faith communications when performing services for the Company.

While no list can capture every situation, examples of conduct you should report include:

- Theft;
- Financial or safety reporting that is fraudulent, misleading, or negligent;
- Improper undocumented financial transactions;
- Forgery or alteration of documents;
- Bribery, collusion, or other corrupt activity;
- Unauthorized alteration or manipulation of computer files;
- Improper destruction of records;
- Improper use of Company property, funds, or other assets;
- Improper access to or use of confidential information;
- Authorizing or receiving payment for goods not received or services not performed; and
- Any other improper matter involving cash, financial procedures, safety, or reporting.

***We Do Not Tolerate Retaliation***

Coming forward with questions or concerns may sometimes feel like a difficult decision, but we are committed to fostering an environment that does not deter individuals from speaking up when they observe conduct that may violate our Code. For that reason, the Company will not tolerate retaliation of any kind because an individual in good faith raises a question or concern about a violation or suspected violation of our Code or because the individual participates in or cooperates with an investigation of such concerns.

Retaliation is any conduct that would reasonably dissuade an individual from raising, reporting, or communicating about good faith concerns through our internal reporting channels or with any governmental authority or from participating in or cooperating with an investigation or legal proceeding raising such concerns.

Retaliation may occur through conduct or written communication and may take many forms, including actual or implied threats, verbal or nonverbal behaviors, coercion, bullying, intimidation, or deliberate exclusionary behaviors.

This protection against retaliation applies even if a concern is ultimately not substantiated, provided it was raised in good faith. A reasonable, good faith belief that a violation may have occurred is enough to warrant reporting.

It is the Company's policy to adhere to all applicable laws protecting individuals against unlawful retaliation or discrimination as a result of their raising good faith questions or concerns. If you are ever aware of an instance or threat of retaliation, please immediately report it. Nothing in this policy prevents the Company from taking appropriate action consistent with the law. In addition, this policy prohibits and does not protect individuals who knowingly and intentionally raise false concerns or reports.

***How to Raise Questions and Concerns***

You can submit your good faith questions or concerns about conduct you believe may violate our Code to:

- The Company employee responsible for administering your engagement with the Company.
- The Human Resources Inbox (HR@lila.ai).
- The Legal Team Inbox (Legal@lila.ai).

Reports may be made orally or in writing, and you do not need to have complete information or certainty that a violation has occurred before raising a good faith concern. Please note that while you may report anonymously, doing so may limit the Company's ability to investigate fully.

When you raise a question or concern, the Company will maintain confidentiality to the fullest extent possible, consistent with applicable legal requirements and the need to conduct an adequate investigation or review.

When raising questions or concerns, we ask that you provide as much detailed information as possible, including the background and history of the concern (e.g., names, dates, times, and locations) and the reasons why the situation is cause for concern.

***What the Company Will Do***

The Company is committed to reviewing all reported concerns, conducting proper, fair, and thorough investigations tailored to the circumstances, and taking appropriate remedial and concluding steps as warranted. All action taken by the Company in response to a concern will necessarily depend on the nature and severity of the concern. This may include initial inquiries and fact-gathering to decide whether an investigation is appropriate and, if so, the form and scope of the investigation. Note that an investigation into concerns raised is not an indication that they have either been confirmed or rejected. The Company complies with the law in conducting investigations and expects that individuals will cooperate with an investigation, except when voluntary compliance with an investigation is requested. Contractors are expected to provide truthful information when participating in an investigation.

## Proprietary Information and Confidentiality

The Company's confidential and proprietary information is vital to its current operations and future success. Contractors should use all reasonable care to protect or otherwise prevent unauthorized access to, disclosure of, or use of such information.

For purposes of this policy, "Proprietary Information" shall have the same meaning as defined in any contractual agreement between the Company and the contractor regarding protection of the Company's confidential and proprietary information.

Proprietary Information does not include conduct that was, or that an individual reasonably believes to be, illegal; conduct that is recognized as against a clear mandate of public policy; or the existence of a non-confidential settlement involving any such conduct. Nothing in this Contractor Handbook prohibits an individual from communicating with any governmental authority or making a report in good faith and with a reasonable belief of any violations of

law or regulation to a governmental authority, or disclosing Proprietary Information which the individual acquired through lawful means in the course of their engagement by the Company to a governmental authority in connection with any communication or report, or from filing, testifying or participating in a legal proceeding relating to any violations, including making other disclosures protected or required by any whistleblower law or regulation to the Securities and Exchange Commission ("SEC"), the Department of Labor ("DOL"), the Office of Federal Contractor Compliance Programs ("OFCCP"), or any other appropriate government authority.

Further, contractors are hereby notified that under the 2016 Defend Trade Secrets Act ("DTSA"): (1) no individual will be held criminally or civilly liable under Federal or State trade secret law for the disclosure of a trade secret (as defined in the Economic Espionage Act) that: (A) is made in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and made solely for the purpose of reporting or investigating a suspected violation of law; or, (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal so that it is not made public; and, (2) an individual who pursues a lawsuit for retaliation by an employer for reporting a suspected violation of the law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court or arbitration proceeding, if the individual files any document containing the trade secret under seal, and does not disclose the trade secret, except as permitted by order in that proceeding.

## Attire and Safety Requirements

Contractors must comply with all applicable safety, laboratory, security, and operational requirements while on Company premises.

Where required by the Company, contractors must wear appropriate personal protective equipment ("PPE"), identification badges, laboratory attire, safety footwear, protective eyewear, gloves, or other safety-related equipment.

Clothing, jewelry, accessories, or personal items that may create a safety, security, contamination, or operational risk may be prohibited in designated areas. Additional site-specific attire requirements may apply to laboratories, manufacturing areas, clean rooms, controlled environments, customer locations, or other restricted areas.

## Social Media and Public Communications

The Company respects the legal rights of its contractors to engage in lawful personal activities and communications. At the same time, contractors performing services for the Company may have access to confidential, proprietary, or non-public information relating to the Company, its employees, customers, suppliers, vendors, business partners, technologies, research activities, and day-to-day operations. Accordingly, the Company has adopted this Social Media and Public Communications Policy to protect such information and prohibit communications by contractors that reasonably could be interpreted as official communications of the Company.

For purposes of this Policy, "social media activity" includes all types of posts and other communications on the internet, including but not limited to, posts on social networking

sites, such as Facebook and LinkedIn; blogs and other on-line journals and diaries; bulletin boards and chat rooms; microblogging, such as X (formerly Twitter); and posts of photographs, video or audio on media-sharing sites, such as YouTube, Instagram, TikTok, or Flickr. "Social media activity" also includes permitting, or failing to remove, posts by others where the individual can control the content of posts, such as on a personal page or blog.

***Scope of This Policy***

This Social Media policy applies:

- To all contractors and contractor personnel providing services to the Company;
- To social media activity using the Company's or personal electronic resources;
- To social media activity that relates in any way to, or may reflect on or impact, the Company's business, employees, customers, business partners, vendors, suppliers, or competitors; and
- Regardless of whether a contractor identifies their contractual affiliation with the Company in their social media activity or in their account profile or posts anonymously or using a pseudonym.

***Guidelines***

- **Know and follow applicable policies and agreements.** A contractor's social media activity is subject to all pertinent Company policies set forth in this Contractor Handbook and in any contractual agreement with the Company.
- **Use of the Company's logo.** Contractors should not use the Company's logo, trademarks, or proprietary graphics in a way that suggests they are representing the Company or while engaging in conduct that violates Company policy.
- **Protect confidential information.** Contractors should not disclose or post images or videos of any of the Company's trade secrets or confidential business information or of any confidential business or manufacturing processes. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Confidential business information may include, but is not limited to, marketing strategies, product launches, pricing policies; plans for the acquisition or disposition of corporate assets, non-public information about customers, and the Company's attorney-client communications.

***Enforcement***

Failure to comply with this policy may result in restriction or revocation of a contractor's facility access, removal of the contractor from Company premises, termination of a

contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

## Contact with the Media

To ensure that the Company communicates with the media in a consistent, timely and professional manner about matters related to the Company, contractors should notify the Chief Communications Officer that they have been contacted by the media whenever they are asked to speak on behalf of the Company so that the Company knows that a media inquiry has been made.

Do not respond to media inquiries on the Company's behalf without authorization.

## Photography and Videography

To protect the Company's confidential and proprietary information, intellectual property, security infrastructure, and personnel privacy, photography and videography are strictly prohibited outside of designated Common Areas with any device capable of capturing or transmitting images or video. This policy applies to employees, temporary employees, visitors, contractors and contractor personnel, and third parties at all Company facilities.

For the purposes of this policy, "Proprietary Information" shall have the same meaning as defined in the Company's Contractor Confidentiality, Assignment, and Non-Solicitation Agreement and the Company's Contractor Confidentiality, Assignment, and Restrictive Covenant Agreement.

For purposes of this policy, "Common Areas" include conference rooms, break rooms, and lobbies. Photography or videography outside of Common Areas requires prior approval from the Chief Communications Officer (CCO) or their designee. Requests may be submitted to press@lila.ai.

- Even within Common Areas, unless prior approval has been obtained, photography and videography must not capture: Proprietary information, trade secrets, or confidential business data
- Intellectual property, including source code, algorithms, formulas, or research
- Computer screens, monitors, whiteboards, or documents containing sensitive information
- Laboratory equipment, testing facilities, or manufacturing processes
- Security equipment or personnel, surveillance cameras, access card readers, badge systems, or other access control technology
- Fire suppression systems, emergency equipment, or evacuation routes
- Any employees, temporary employees, visitors, or third parties

Contractors who host visitors or third parties are responsible for ensuring their guests comply with this policy.

***Content Publishing from Authorized Photography and Videography***

CCO approval is required prior to external publishing of any content in any form or medium, whether electronic, print, social media (e.g., Facebook, LinkedIn, X Instagram) or otherwise. The Company reserves the right to delete, restrict, or prohibit any content from external distribution if necessary to protect its legitimate business interests.

***Violations***

Violations of this policy should be reported to the CCO at press@lila.ai or to the Chief Information Security Officer (CISO) at security@lila.ai. Visitors and third parties who violate this policy may be removed immediately and barred from future access. Failure to comply with this Policy may lead to device confiscation, deletion of captured content, and forensic analysis of the device content was captured on. For contractors, violation of this policy may also result in restriction or revocation of facility access, removal from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

# WORKPLACE SAFETY AND SECURITY

## Anti-Violence Policy

The safety and security of our workplace is of vital importance to the Company. Therefore, the Company has adopted a zero-tolerance policy concerning work-related violence. Threats or acts of violence—including intimidation, bullying, physical or mental abuse and/or coercion—will not be tolerated.

It is our goal to have a work environment free from acts or threats of violence and to respond effectively in the event that such acts or threats of violence do occur.

Work-related violence is any intentional conduct that is sufficiently severe, abusive, or intimidating to cause an individual to reasonably fear for their own personal safety or the safety of their family, friends, and/or property such that employment conditions are altered or a hostile, abusive or intimidating work environment is created for one or more employees. The conduct prohibited by this policy applies to conduct by all persons involved in our operations, including employees, managers, temporary or seasonal employees ("employees"), contractors and contractor personnel, agents, clients, vendors, customers, or any other third-party interacting with the Company ("third parties").

Examples of work-related violence include, but are not limited to:

- Threats or acts of violence occurring on Company premises, regardless of the relationship between the parties involved in the incident.

- Threats or acts of violence occurring off Company premises involving someone who is acting in the capacity of a representative of the Company.

- Threats or acts of violence occurring off Company premises involving an employee if the threats or acts affect the business interests of the Company.

- All threats or acts of violence occurring off Company premises, of which an employee is a victim, if we determine that the incident may lead to an incident of violence on Company premises; and

- Threats or acts of violence resulting in the conviction of an employee or agent of the Company, or an individual performing services for the Company on a contract or temporary basis, under any criminal code provision relating to violence or threats of violence when that act or the conviction adversely affects the legitimate business interests of the Company.

Examples of conduct that may be considered threats or acts of violence under this policy include, but are not limited to:

- Threatening physical contact directed toward another individual.

- Threatening an individual or the individual's family, friends, associates, or property with harm.

- The intentional destruction or threat of destruction of the Company's or another's property.

- Menacing or threatening phone calls.

- Stalking.

- Veiled threats of physical harm or similar intimidation; and/or

- Communicating an endorsement of the inappropriate use of firearms or weapons.

Work-related violence does not refer to work environment arguments or debates that are zealous or impassioned, provided there is no resort to any form of coercion. Discussions about sporting activities, popular entertainment or current events are not considered work-related violence when there is no threat of violence being directed to the work environment or any individual connected with it. Rather, work-related violence refers to behavior that demonstrates an intention to engage in violence, condones violence in our work environment, or targets any individual with acts or threats of violence.

Contractors play an important role in helping the Company to maintain a violence-free work environment. To that end, contractors are encouraged to immediately report any incident that violates this policy to the Company contact responsible for administering the contractor's engagement for the Company.

## Anti-Bullying Policy

The Company does not tolerate bullying behavior, as explained in this policy.

Work-related bullying is the use of force, threats or coercion to abuse, intimidate, or humiliate another individual. Workplace bullying includes, but is not limited to, the following:

- Verbal abuse, such as the use of patently offensive, demeaning, or humiliating remarks and epithets.
- Verbal or physical conduct that is threatening or obscene.
- Pushing, shoving, kicking, poking, tripping, assaulting, or threatening physical assault, or intentionally damaging a person's work area or property; or
- Sabotage, or deliberately subverting, obstructing or disrupting another person's work performance.

Cyberbullying is also prohibited. Cyberbullying refers to bullying, as defined above that occurs through the use of a computer, cell phone, smartphone, tablet, or other device that transmits electronic information, regardless of whether the device is owned by or located at the Company or connected to the Company network.

***Reporting and Response***

Contractors who are subject to, or witness, bullying in our work environment are encouraged to notify the Company contact responsible for administering the contractor's engagement for the Company immediately.

The Company will promptly investigate the complaint. The Company will maintain confidentiality to the extent possible, consistent with its commitment to investigating the complaint promptly and thoroughly.

If the complaint is verified, the Company will take appropriate action. For contractors, this may include restriction or revocation of facility access, removal from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

The Company will also report to law enforcement, if appropriate. The complaining party will be advised of the results of the investigation.

***Anti-Retaliation***

The Company prohibits retaliation against an individual for making a good faith claim of bullying or for participating in good faith in an investigation of bullying.

## Weapons in the Workplace

***Scope and Applicability***

The Company is committed to maintaining a safe and secure workplace. This policy establishes guidelines for weapons on Company property to minimize security risks and applies to all employees, contractors and contractor personnel, vendors, visitors, and other persons on Company property. Company property is defined as all physical space owned,

leased, or occupied by the Company. This includes but is not limited to offices, meeting rooms, kitchens, break areas, and common areas. Unless this policy is contrary to state or local law, the workplace specifically includes Company parking areas.

Furthermore, where the Company operates as a tenant, contractors must comply with facility requirements, policies, and landlord restrictions in addition to this policy. When applicable law, local ordinances, or facility polices are stricter than this policy, the stricter requirement applies.

***Legal Hierarchy***

This policy is subject to applicable law wherein the following hierarchy applies:

- Local ordinances and city regulations
- State law
- Federal law
- Facility Owner Requirements and Policies

***General Prohibition***

The Company prohibits any person providing services to the Company or located on the Company's premises from possessing weapons of any kind at the workplace with specific exceptions. Contractor. This policy prohibits the possession of concealed weapons as well as weapons carried openly. Specific exceptions to this policy are covered under the Permitted Items and Authorized Security and Executive Protection sections.

This prohibition specifically includes guns, rifles, and firearms of any type, including those for which the holder has a legal permit. Other examples of prohibited weapons include, but are not limited to, knives, ammunition, explosives, bombs, bows and arrows, clubs, slingshots, blackjacks, metal knuckles, fixed blade knives, pocket knives, tasers, stun guns, weapons capable of ejecting a projectile (e.g., rubber bullet gun), and similar devices that by their design or intended use can inflict serious bodily injury or lethal force.

***Permitted Items, Authorized Security and Executive Protection***

The only weapon permitted without additional approval is pepper spray (aerosol or gel). Pepper spray may be carried on company property *if and only if* the following requirements are met:

- The pepper spray is legal to possess and carry in your jurisdiction (local, state, and/or federal law);
- The container size complies with limits set by federal, state, and local law;
- The container is securely stored and not visible during work hours (concealed on person or in a personal bag, locker, or closed container); and

- The employee assumes full responsibility for the item.

For authorized security personnel and executive protection, firearms and weapons relevant to job duties may be carried *if and only if* the following requirements are met:

- The individual has been explicitly authorized by the CEO or President of Business Operations;
- The authorization is documented in writing;
- The individual holds all required licenses, certifications, and permits under applicable law;
- The individual has completed relevant security training as required by the Company
- The individual has completed all relevant training as required under the law of the jurisdiction they work in; and
- The weapon complies with all applicable local, state, and federal law

All authorized weapons must be carried concealed and handled in accordance with applicable law and the Company's security protocols.

***Contractor Responsibility***

Any item brought onto Company property must be compliant with this policy and all applicable local, state, and federal law as well as facility policies. Ignorance of the law is not an excuse for policy violation. When in doubt, consult with Protective Security and Legal before bringing any item to work.

***Reporting and Enforcement***

Maintaining a safe workplace is a shared responsibility. Contractors should promptly report any weapon, threat, policy violation, or situation that creates a safety concern. In an emergency or any situation involving an immediate threat, call your local emergency number first, and then notify Protective Security. If you see or find a weapon, do not touch or handle it; keep yourself and others away and contact building security or Protective Security immediately.

Reports and questions may be submitted through any of the following channels:

- Email Company Security (security@lila.ai)
- Submit the incident form in the IT Support Portal;
- Contact building security for your facility;
- The Company contact responsible for administering your engagement for the Company.

All reports are taken seriously and handled as confidentially as possible in coordination with building management and law enforcement as needed. The Company prohibits retaliation against anyone who makes a good-faith report.

Any violation of this policy, accidental discharge, display, or misuse will be investigated and may result in termination of the contractor's engagement with the Company, removal from Company property, and referral to law enforcement.

## Work-Related Injuries

The Company is committed to maintaining a safe work environment for all individuals performing services on its premises. Any contractor who sustains a work-related injury or illness should inform the Company contact responsible for administering their engagement immediately. No matter how minor an on-the-job injury may appear, it is important that it be reported immediately.

Nothing in this policy alters the contractor's independent contractor relationship with the Company or creates any entitlement to employee benefits, including workers' compensation benefits. Contractors are responsible for maintaining any insurance coverage required under their contractual arrangements with the Company and should direct questions regarding insurance coverage, claims, or benefits to their employer, insurer, or other responsible party, as applicable.

## Smoke-Free Workplace

The Company provides a work environment that is smoke-free. Smoking and the use of all tobacco-related products, including, but not limited to, smoking, the use of chewing tobacco or other smokeless tobacco and the use of e-cigarettes or vaping, is prohibited inside the building. Contractors who observe others smoking or using tobacco products in the workplace have a right to object and should report the violation to the Company contact responsible for administering their engagement.

Smoking, vaping, consuming or otherwise possessing cannabis on the Company's premises is prohibited, including in designated smoking areas. Contractors should refer to the Company's Drug- and Alcohol-Free Work policy.

## Drug- and Alcohol-Free Workplace Policy

### *Purpose*

The Company is dedicated to providing a workplace that is safe, healthy, and free of drugs and alcohol. Continuing research and practical experience have proven that even limited quantities of illegal drugs, abused prescription drugs or alcohol can impair reflexes and judgment. This Impairment, even when not readily apparent, can have catastrophic consequences. Moreover, studies have shown that Impairment by Controlled Substances may last long after the user believes the effects to have worn off.

***Scope and Applicability***

Contractors and contractor personnel have a responsibility to perform their services to the Company in a safe and conscientious manner and to comply with the Company's safety and security requirements. As such, this policy covers situations such as but not limited to:

- Time spent on Company Premises and at Company Sponsored Events.
- Performance of services for or on behalf of the Company.
- Operation of any Company equipment or vehicles.

***Definitions***

- *Controlled Substance*: Any drug or substance regulated under the federal Controlled Substances Act or applicable state law, including prescription drugs used without a valid prescription, outside prescribed parameters, or illegally or improperly obtained.
- *Impairment*: A diminished ability to safely perform services due to the use of alcohol, Controlled Substances, or other intoxicants, whether or not the cause of impairment is visually apparent.
- *Safety-Sensitive Role*: Any position in which the contractor operates a Company vehicle, transports personnel, provides executive protection, or performs functions where Impairment could cause direct harm to people or property. Includes but is not limited to Executive Driver, Protective Security Detail, and courier roles.
- *Company Premises*: All locations owned, leased, or operated by the Company, including parking areas, common areas, and any offsite facility at which the Company is conducting business.
- *Company-Sponsored Event*: Any event organized, funded, or formally sanctioned by the Company, whether held on or off Company Premises.
- *Reasonable Suspicion*: A belief based on specific, articulable, contemporaneous observations that an individual may be impaired, including but not limited to slurred speech, unsteady gait, odor of alcohol, erratic or aggressive behavior, or altered mental status.

***Drug Use/Distribution/Possession/Impairment***

The Company prohibits the use, sale, attempted sale, conveyance, distribution, manufacture, purchase, attempted purchase, possession, cultivation and/or transfer of illegal drugs or other unlawful intoxicants at any time, and in any amount or any manner, regardless of occasion. "Illegal drugs" means all drugs whose use or possession is regulated or prohibited by federal, state, or local law, and include Controlled Substances.

Unless otherwise limited by state law, the Company prohibits the use of marijuana and marijuana products. Contractors may not be impaired while performing services for the Company due to the use of medical or recreational marijuana or if marijuana or marijuana products are brought onto Company property or in Company-provided vehicles.

***Alcohol Use/Distribution/Possession/Impairment***

Contractors are prohibited from distributing, dispensing, possessing, or using any beverage or medicine containing alcohol while performing services for the Company or on Company Premises and from performing services for the Company with alcohol in their systems.

The Company's prohibition of alcohol use while on Company Premises does not apply to consumption of alcohol that is expressly made available by the Company at Company-Sponsored Events, provided consumption is lawful, moderate, and does not result in Impairment. The Company reserves the right to restrict or discontinue the availability of alcohol on Company Premises at any time.

In all cases, the Company strictly prohibits the consumption, distribution, or possession of alcohol by any individual under the local minimum legal drinking age.

***Reasonable Suspicion and Reporting***

Contractors are expected to promptly report any suspected violation of this policy. Violations of this policy should be reported to the Company contact responsible for administering the contractor's engagement.

Reporting of violations includes and allows for Reasonable Suspicion of Impairment. Reasonable suspicion of Impairment may be based on observable indicators, including but not limited to the odor of alcohol, slurred speech, unsteady gait, erratic behavior, or altered mental state.

***Prescription and Over-the-Counter Drugs***

This policy does not prohibit the possession and proper use of lawfully prescribed or over-the-counter drugs. However, contractors taking medication should consult with a health care professional or review dosing directions for information about the medication's effect on the contractor's ability to work safely and promptly disclose any work restrictions to the Company contact responsible for administering their engagement. Contractors are not required to reveal the name of the medication or the underlying medical condition.

***Safety Sensitive Roles***

Contractors providing services to the Company in Safety-Sensitive Roles may be subject to additional requirements, which may include pre-employment, reasonable suspicion, post-incident, return-to-duty, and follow-up drug and alcohol testing. This is necessary to further ensure workplace safety given sensitivity to these roles.

***Consequences of Policy Violations***

Violation of this policy will result in investigation and may result in removal of the individual from Company Premises, suspension or revocation of access to Company facilities or systems, or termination of the contractor's engagement with the Company.

may be required prior to returning to work and as part of an incident investigation.

Where a policy violation involves threatening behavior, physical aggression, or a public safety concern, the Protective Security team and/or law enforcement may be engaged, as appropriate.

## Company's Right to Search

The Company wishes to maintain a work environment that is free of illegal drugs, alcohol, firearms, explosives, or other improper materials. To this end, the Company prohibits the control, possession, transfer, sale, or use of such materials on its premises to the extent permitted by applicable law. We require the cooperation of all individuals performing services on the Company's premises in administering this policy.

Desks, lockers, and other storage devices may be provided for the convenience of contractors providing services to the Company, but they remain the sole property of the Company. Contractors have no reasonable expectation of privacy for items placed therein. Accordingly, desks, lockers, and other storage devices, as well as any articles found within them, can be inspected by any agent or representative of the Company at any time, upon reasonable suspicion, either with or without prior notice.

The Company is charged with a duty to protect its employees and others from injuries at the hands of individuals who pose a known risk of bodily harm to others. Accordingly, to ensure the safety and security of those individuals and to protect our legitimate business interests, we reserve the right, upon reasonable suspicion, to question, inspect, or search any individual entering or leaving Company premises or job sites. The inspection or search may include any packages or items that the individual may be carrying, including briefcases, handbags, backpacks, and shopping bags.

These items are subject to inspection and search, upon reasonable suspicion, at any time, with or without prior notice. Contractors may be required to consent to reasonable inspection of their personal property and/or person while performing services for the Company on the Company's premises, to the extent permitted by applicable law. Any inspection of an individual's person will be limited to a self-inspection, whereby they will be requested to self-inspect their personal property or person by displaying the contents of any packages and/or turning out their pockets, etc., in the presence of a representative of the Company, typically a management employee of the same sex or gender.

For the purposes of this policy, reasonable suspicion is defined as specific and articulable facts, taken together with rational inferences from those facts, that the individual is in possession of drugs, contraband, or other illegal materials.

## Use of Company Equipment and Resources

When using Company equipment, vehicles, or other property, contractors are expected to exercise reasonable care, maintain the property in safe working order, and follow all operating instructions, safety standards, and guidelines provided to them by the Company.

Contractors should notify the Company employee responsible for overseeing their engagement if any equipment, machines, tools, or vehicles appear to be damaged, defective, or in need of repair. Prompt reporting of damages, defects, and the need for

repairs could prevent deterioration of equipment and injury to others. Contractors who have questions about their responsibility for maintenance and care of equipment or vehicles used while performing services for the Company should consult the Company employee responsible for overseeing their engagement.

Contractors are expected to comply with all local, state, and federal laws while operating Company vehicles and other equipment.

## Business Equipment and Information Systems Usage Policy

The Company has significantly invested in telephone services, copiers, computers, laptops, tablets, mobile phones, messaging systems, hardware, internet access, e-mail, software, networks, computer accounts, data storage, voicemail, AI-powered systems and all other types of business equipment and electronic resources provided by the Company or connected to the Company's network or used at a Company site (collectively "Business Equipment and Information Systems"). The Company's Business Equipment and Information Systems are vital to keeping our operations flowing smoothly and effectively. This policy clearly outlines expectations for the use of the Company's Business Equipment. It is designed to help safeguard our integrity and maintain trust.

***Monitoring of Business Equipment and Information Systems; No Expectation of Privacy***

The Business Equipment and Information Systems provided by the Company, and all information and electronic communications transmitted through, received by or stored on the Business Equipment or Information Systems, are the exclusive property of the Company.

The Company (and/or through its authorized representatives) has the right, without notice, in its sole discretion, to monitor, review, retain, disclose and/or take any other appropriate actions regarding (collectively, "Monitoring") any information and electronic communications transmitted through, received by or stored on its Business Equipment and Information Systems – including e-mails and messages sent or received (whether such e-mails and messages are related to personal or business matters and/or whether they are sent or received using a Company mail account, a non-Company internet-based account, such as yahoo.com, hotmail.com, gmail.com, or a social networking website), faxes, voicemails, internet and Intranet communications, access and usage, and documents, files or programs stored on the Company's Business Equipment and Information Systems to the fullest extent permitted by law. The Company's rights regarding Monitoring use of the Business Equipment and Information Systems exist whenever an individual uses the Company's Business Equipment and Information Systems. Thus, at no time should individuals believe that they have any expectation of privacy while using any of the Company's Business Equipment and Information Systems.

Contractors' use of the Company's Business Equipment and Information Systems constitutes their consent to Monitoring by the Company (and/or its authorized representatives). Therefore, individuals should not expect privacy or confidentiality in anything they create, download, display, store, send or receive on the Company's Information Systems, even if it has been deleted, password-protected, encrypted or is marked "confidential," "private," "personal," "privileged" or other words or phrases intended to convey it is private. In addition, the use of passwords to gain access to the

Company's Business Equipment and Information Systems is intended solely to protect the security of the Company's business and does not confer an expectation of privacy. If an individual wishes to avoid having the Company potentially accessing and reviewing their personal communications, documents, files, or data, then they should not use the Company's Business Equipment and Information Systems for personal purposes and should not save personal material on the Company's Business Equipment and Information Systems.

***Acceptable Use Policy - BIZ-IT-SEC-001***

The Company maintains an Information Security Management System (ISMS) and an associated suite of information security policies of which the Acceptable Use Policy (BIZ-IT-SEC-001) is the governing policy. The current, approved versions of these policies are maintained by the IT & Security team in the Company policy library (SharePoint) and are communicated through this handbook and directly to personnel from time to time.

The Company's Business Equipment and Information Systems are provided for the benefit of the Company's business. Contractors may use Company e-mail for personal use, provided such use complies with Company rules and policies, and applicable laws. Contractors should never use the Company's Business Equipment and Information Systems for personal use in a manner that degrades the functionality of those systems or interferes with the services that they are providing to the Company.

The following guidelines, which are not all-inclusive, have been established to ensure that individuals understand expectations regarding use of the Company's Business Equipment and Information Systems:

- General Guidelines
    - Sending, saving, accessing, or viewing obscene or vulgar material on the Company's Business Equipment and Information Systems is prohibited. Messages stored and/or transmitted by the Company's Business Equipment and Information Systems must not contain content that may reasonably be considered to be obscene or other patently offensive material, including but not limited to, sexual comments, jokes or images; racial slurs; gender-specific comments; or any comments, jokes or images that would discriminate against or harass someone on the basis of their race, color, sex, age, national origin or ancestry, disability, or any other category protected by federal, state or local law. Any use of the Company's Business Equipment and Information Systems to engage in harassment or discrimination prohibited by Company policies is unlawful and prohibited.
    - The Company's policies apply fully to the use of the Company's Business Equipment and Information Systems. Any use of the Company's Business Equipment and Information Systems that violates a Company policy is prohibited.
    - The Company's Business Equipment and Information Systems must not be used for solicitation purposes while performing services for the Company. The

Company's no solicitation rule applies to the use of the Company's Business Equipment and Information Systems.

- Contractors may use software on local area networks or on multiple machines only in accordance with applicable license agreements.
- Contractors may not download software and install it on Company Business Equipment and Information Systems. The Company reserves the right to audit any Company computer or equipment to determine what software is installed on the local drive(s).
- Contractors may not use Company systems for personal business ventures.
- If a contractor has a dedicated desk at a Company worksite, they must clear any sensitive documents and credentials from their desk when unattended and at day's end.
- Contractors must comply with all applicable export-control laws and regulations when sharing, transmitting, or transferring technical data, software, or source code.
- If documents must be printed, documents containing confidential information must be shredded.

- Accounts, Credentials, and Authentication Guidelines
  - Contractors must comply with the password and other security provisions of the Company's Business Equipment and Information Systems.
  - Contractors must not use codes or passwords to gain unauthorized access to files.
  - Contractors must not provide access to the Company's Business Equipment and Information Systems to anyone other than employees of the Company or contractor personnel who are authorized users.
  - Contractors must keep their credentials private. Contractors may not share them or use aliases to conceal their identity or actions.
  - Contractors must use the Company-approved password manager. Contractors may not write credentials down or store them in unsecured locations or tools such as Slack, Microsoft Teams, or SharePoint.
  - Contractors must obtain IT & Security approval before creating accounts or adopting new software, platforms, or cloud services.

- Devices and Asset Handling
  - Contractors are responsible for the security of their Company-issued equipment whether in the office, at home, or remote.

- Contractors must lock devices when unattended and store them securely.
- Contractors may not tamper with device-management tools or security features such as firewalls, updates, or endpoint protection.
- Contractors must obtain prior approval before using external storage (e.g., USB Drives); approved devices must be encrypted.
- Contractors must return all Company-issued equipment, badges, and property when their employment ends.
- Contractors must report lost or stolen devices immediately.

- Remote Work
  - Contractors must use Company-approved devices and tools; personal devices used for work must meet basic security standards and limit company-data storage.
  - Contractors must avoid storing sensitive Company data locally unless necessary. Furthermore, they must remove local data when it is no longer needed.
  - Contractors must use the VPN over public, shared, or unsecured networks.
  - Contractors are expected, to the best of their ability, to keep their devices and home networks patched.

- Network Use
  - Contractors may not take any action that disrupts or degrades the Company's systems, networks, or services, including denial-of-service (DoS) attacks or packet spoofing.
  - Contractors may not use packet sniffers, honeypots, or similar tools without prior IT & Security approval.
  - Contractors may not install unauthorized network devices
  - Contractors may not introduce malicious code
  - Contractors may not perform security or vulnerability scans without prior approval from IT & Security (e.g., port scans, penetration tests, automated vulnerability assessments, etc.).

Violations of this policy, suspicious activity, or suspected security incidents should immediately be reported to IT & Security (security@lila.ai).

***Computer and Systems Security***

All Company Business Equipment and Information Systems and the data stored on them are, and remain at all times, the property of the Company. As such, all messages created, sent, or retrieved over the internet or the Company's Business Equipment and Information Systems are the property of the Company, and should be considered Company information. The Company reserves the right to retrieve and read any message composed, sent, or received using the Company's Business Equipment and Information Systems for any business reason, including, but not limited to, ensuring compliance with this and all Company policies.

Contractors should be aware that even when a message is deleted or erased, it is still possible to re-create the message; therefore, ultimate privacy of a message cannot be ensured to anyone. Accordingly, internet, email and other messages are not private. Furthermore, all communications, including, but not limited to, text and images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Contractors should also be aware that duplicates of email or other messages transmitted through a personal, web-based email account using Company equipment could be stored on the Company's Business Equipment and Information Systems; likewise, information regarding internet sites that an individual has accessed may also be stored.

***Email and Message Content Screening***

The Company maintains the right to screen all inbound and outbound email and other message (*e.g.*, instant messages) content sent or received on the Company's Business Equipment and Information Systems. Messages or attachments that contain obscene or vulgar material may be quarantined and held from transmission or receipt until the sender or recipient can verify the message or attached document is work-related.

If an individual wants to communicate with an attorney or send an otherwise confidential piece of communication that they do not want the Company to monitor, they should consider using a personal email address and personal computer equipment. If an individual uses Company Business Equipment or Information Systems, they consent to any monitoring by the Company and should understand that there is no right to privacy with respect to such communications, to the extent permissible under applicable law.

***Virus Protection***

To prevent computer viruses from being transmitted through the system, individuals are not authorized to download any software from the internet onto any Company Business Equipment or Information Systems.

The Company maintains virus protection software on all network servers and filters all inbound and outbound email for virus attachments. Email containing a virus will be quarantined and both the sender and recipient will be informed. If the virus can be removed, the message will be forwarded to the recipient.

### *Discipline*

Violation of this policy may result in restriction or revocation of the contractor's facility access, removal of the contractor from Company premises, termination of a contractual relationship, or other action deemed appropriate by the Company, in its sole discretion.

## No Solicitation/Distribution of Literature

Contractors are not permitted to solicit or to distribute written material for any purpose on Company property at any time.

## Physical Security (BIZ-IT-SEC-015)

The Company is committed to maintaining a safe and secure physical environment across all its facilities. Physical security controls are in place to protect our employees, research assets, and confidential information from unauthorized access, theft, misuse, and environmental threats. All employees, contractors and contractor personnel, and visitors are expected to comply with applicable physical security requirements at every Company location. The Company's physical security program is organized around four areas: access control, physical environment protection, visitor and third-party management, and incident response. These controls are designed to comply with applicable legal requirements and align with industry security standards including ISO 27001 and SOC 2.

### *Physical Security Permitting*

Company offices and processing facilities meet applicable local building codes for the construction of walls, windows, doors, and access-control mechanisms. Certain interior zones are designated as secure areas where physical access is further restricted to a subset of authorized personnel.

### *Access Control*

Access to Company facilities is controlled through a centralized electronic access system with granular, per-person control. Contractors performing services on-site at a Company worksite will be issued unique access credentials that may not be shared, loaned, or transferred. Credentials must be presented to enter secured areas. Tailgating — entering a secured area by following another person without using one's own credential — is prohibited.

Where possible, access-control systems are tied to a centralized system that provides granular access control for individual personnel. Access events are logged and reviewed as needed according to risk.

Lost, stolen, or damaged credentials must be reported to the Protective Security team immediately. Access rights are provisioned based on role and business need. Access rights are reviewed and updated upon changes in status, role, or site assignment. Access to sensitive or restricted areas requires additional authorization.

***Visitors and Third-Party Management***

Restricting access to Company premises helps maintain safety standards, protect against theft, ensure security of equipment, protect confidential information, safeguard general welfare, and avoid potential distractions and disturbances. For this reason, only authorized visitors are allowed in the workplace and all authorized visitors, including but not limited to friends, family, third party vendors, and former associates are required to sign in upon arrival, be issued a visitor credential and must be escorted at all times by a Company employee when in secured areas.

Contractors entering a Company worksite must sign in and out on a visitor log and must be escorted or monitored by Company personnel while in secure areas of the worksite. Contractor access to secure areas must be confirmed with the appropriate Company personnel before access is granted. Contractors may work unescorted only when the sponsoring employee can ensure the contractor will not have unauthorized access to Company information systems, networks, or data.

Contractors must comply with the Company's physical security and environmental control requirements. The Company assesses the adequacy of third-party physical security controls as part of its vendor management process.

The Company reserves the right to verify the contents of packages, bags, and briefcases brought onto Company premises by contractors.

***Secure Areas and Environmental Controls***

Certain areas within Company facilities are designated as secure or restricted zones. Access to these areas is limited to authorized personnel only. Secure areas are monitored through video surveillance, intrusion detection systems, and other appropriate controls. Cameras and intrusion-detection systems are used at facilities that store or process production or sensitive internal Company data. Contractors must not prop open secured doors, disable access control mechanisms, or otherwise circumvent physical security controls.

Facilities housing sensitive systems or data are equipped with appropriate environmental safeguards including fire suppression, climate monitoring, and emergency power systems. Physical security hardware and supporting infrastructure are maintained in accordance with manufacturer recommendations.

***Delivery and Loading Areas***

Access points such as delivery and loading areas and other points where unauthorized persons could enter secure areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

***Supplier, Vendor, and Third-Party Security***

Suppliers, vendors, and third parties shall comply with the Company's physical security and environmental controls requirements.

The Company shall assess the adequacy of third-party physical security controls as part of the Vendor management process, in accordance with the Third-Party Management Policy.

***Reporting Security Concerns***

Contractors are expected to report any physical security concerns, suspicious activity, unescorted visitors, or observed policy violations to the Protective Security team promptly. This includes, but is not limited to, unauthorized individuals in secured areas, tampered or malfunctioning access control equipment, and any situation that creates a risk to the safety or security of people or property.

***Violations and Enforcement***

Violations of physical security requirements may result in suspension or revocation of a contractor's privileges to access Company facilities and networks or termination of the contractor's engagement. Violations may be reported to law enforcement where appropriate. Known violations should be reported to the Chief Information Security Officer (CISO). Exceptions to physical security requirements must be submitted to and approved by the CISO in advance.

Exceptions to this policy require approval from the CISO in advance. This policy is reviewed periodically and updated as needed. Questions about this policy or requests to report a concern should be directed to the Protective Security team (security@lila.ai).