CODE OF CONDUCT

Document Version: 1.0

Effective Date: [Insert Date]

Prepared By: Human Resources Department

Approved By: Executive Management

1. Purpose

The purpose of this Code of Conduct is to define the ethical standards, professional expectations, and behavioral principles that guide all employees, contractors, and representatives of **Unosecur**.

Unosecur is committed to conducting business with the highest level of integrity, professionalism, and legal compliance. This code establishes the behavioral framework that supports a culture of ethical decision-making and responsible conduct across all areas of the organization.

This policy is designed to:

- Promote ethical and lawful business practices
- Establish clear behavioral expectations for employees
- Protect the confidentiality and integrity of company and customer information
- Maintain a respectful and inclusive workplace environment
- Ensure compliance with applicable laws and regulations
- Support the protection of intellectual property and technological assets

Employees at all levels of the organization are expected to uphold the principles described in this document and to act in a manner that reflects positively on Unosecur's reputation, operations, and long-term objectives.

2. Scope

This Code of Conduct applies to all individuals associated with Unosecur, including but not limited to:

- Full-time employees
- Part-time employees
- Contract employees
- Consultants and advisors
- Interns and trainees
- Vendors or third parties representing Unosecur in business activities

The principles outlined in this policy apply in all professional situations where an individual represents or interacts on behalf of the company, including:

- Office environments
- Remote and hybrid work environments

- Client meetings and business interactions
- Conferences and professional events
- Business travel
- Digital communication platforms
- Social media when representing the company

All individuals covered by this policy are responsible for understanding and complying with its provisions.

Managers and leadership personnel carry additional responsibility to model ethical behavior, ensure awareness of this policy within their teams, and take appropriate action when violations occur.

3. Organizational Values

The values of Unosecur form the ethical foundation upon which all business decisions and workplace behaviors are built. Employees are expected to demonstrate these values in their daily work and interactions.

3.1 Integrity

Integrity is the cornerstone of trust within the organization and with external stakeholders.

Employees must conduct business honestly, transparently, and responsibly. Misrepresentation of facts, manipulation of data, or intentional deception is strictly prohibited.

Employees must always act in a way that preserves the credibility and ethical standing of the organization.

3.2 Respect

Respect for individuals is fundamental to maintaining a productive and inclusive workplace.

Employees must treat colleagues, partners, customers, and stakeholders with dignity, professionalism, and courtesy regardless of differences in role, background, or perspective.

Constructive disagreement is encouraged, but disrespectful behavior, hostility, or personal attacks are unacceptable.

3.3 Accountability

Every employee is responsible for their actions, decisions, and professional conduct.

Accountability means acknowledging mistakes, correcting them promptly, and learning from experience. Employees must take ownership of their responsibilities and follow established policies and procedures.

3.4 Innovation

Unosecur values curiosity, creativity, and continuous improvement.

Employees are encouraged to develop new ideas, explore innovative approaches, and contribute to the advancement of the company's technological capabilities.

Innovation must always occur within ethical, legal, and security boundaries.

3.5 Customer Trust

As a company operating in the technology and security domain, maintaining customer trust is essential.

Employees must protect customer information, deliver reliable services, and maintain the highest standards of confidentiality and professional responsibility.

Trust is built through consistent, ethical behavior and reliable service delivery.

4. Professional Conduct

Professionalism is expected in all workplace interactions and business activities.

Employees are required to perform their duties in a manner that reflects competence, responsibility, and respect for others.

Professional conduct includes:

- Completing assigned responsibilities in a timely and reliable manner
- Communicating clearly and respectfully with colleagues and stakeholders
- Collaborating effectively with team members
- Following internal policies, procedures, and security standards
- Maintaining appropriate workplace etiquette

Employees must avoid behavior that disrupts workplace harmony or damages the organization's professional environment.

Examples of unacceptable conduct include:

- Verbal abuse or aggressive behavior
- Intimidation or threats
- Spreading false information about colleagues
- Deliberate obstruction of team collaboration
- Any behavior that undermines workplace morale or safety

Employees representing Unosecur externally must maintain the same professional standards when interacting with clients, partners, vendors, and the broader community.

5. Compliance with Laws and Regulations

Unosecur is committed to full compliance with all applicable laws, regulations, and industry standards in the jurisdictions where it operates.

Employees must adhere to all relevant legal and regulatory requirements, including but not limited to:

- Data protection and privacy regulations
- Cybersecurity and information protection laws
- Intellectual property regulations
- Anti-corruption and anti-bribery laws
- Employment and labor laws
- Technology export and compliance regulations

Employees must not engage in activities that violate legal or regulatory requirements or expose the company to legal liability.

Any employee who becomes aware of a potential legal violation must promptly report the issue through the appropriate reporting channels described in this policy.

Failure to comply with applicable laws or regulations may result in disciplinary action, including termination of employment and potential legal consequences.

6. Workplace Respect and Anti-Harassment

Unosecur is committed to maintaining a workplace that is safe, respectful, and free from harassment or discrimination.

Harassment of any form undermines workplace dignity and productivity and is strictly prohibited.

Harassment includes any unwelcome behavior that creates an intimidating, hostile, or offensive work environment.

Examples include:

- Sexual harassment
- Bullying or intimidation
- Verbal abuse or offensive language
- Threatening behavior
- Persistent unwanted attention or advances

Discrimination against individuals based on personal characteristics is also strictly prohibited.

Protected characteristics include, but are not limited to:

- Gender or gender identity
- Race or ethnicity
- Religion or belief
- Age
- Disability
- Sexual orientation
- National origin

All employees are responsible for contributing to a respectful and inclusive workplace environment.

Managers have an additional obligation to address inappropriate behavior promptly and escalate issues to Human Resources when necessary.

Employees who experience or witness harassment or discrimination are encouraged to report the incident through the reporting channels defined in this policy. Reports will be handled confidentially and investigated appropriately.

Retaliation against individuals who report concerns in good faith will not be tolerated.

7. Diversity, Equity, and Inclusion

Unosecur believes that a diverse and inclusive workplace strengthens innovation, creativity, and decision-making.

Employees from different backgrounds bring unique experiences, perspectives, and ideas that improve the organization's ability to solve complex problems and develop innovative technology solutions.

Unosecur is committed to providing equal opportunity in all aspects of employment, including:

- Recruitment and hiring
- Promotions and career development
- Compensation and benefits
- Training opportunities
- Workplace participation

Employees must treat colleagues fairly and without bias. Discriminatory behavior, exclusion, or unfair treatment based on personal characteristics is strictly prohibited.

Employees are encouraged to foster an environment that promotes collaboration, openness, and mutual respect. Diversity must be viewed as an organizational strength rather than a challenge.

Managers and leadership personnel are responsible for ensuring that hiring and workplace practices remain fair, transparent, and inclusive.

8. Conflict of Interest

Employees must avoid situations in which personal interests interfere, or appear to interfere, with the interests of Unosecur.

A conflict of interest may occur when an employee's personal, financial, or external professional activities influence their ability to perform their responsibilities objectively.

Examples of conflicts of interest include:

- Holding financial interests in a competitor or vendor
- Accepting gifts, benefits, or favors that influence decision-making
- Working for a competing organization while employed by Unosecur

- Using company information or opportunities for personal benefit
- Hiring or supervising close family members without disclosure

Employees must promptly disclose any potential or actual conflict of interest to management or the Human Resources department.

The organization will review the disclosed situation and determine appropriate actions to eliminate or mitigate the conflict.

Failure to disclose conflicts of interest may result in disciplinary action.

Transparency protects both the employee and the organization from ethical and legal complications.

9. Confidentiality and Data Protection

Employees may have access to confidential, proprietary, or sensitive information during the course of their work.

Protecting this information is essential to maintaining customer trust, protecting intellectual property, and complying with regulatory obligations.

Confidential information may include:

- Customer data and records
- Product source code and system architecture
- Security designs and vulnerability information
- Financial data and internal reports
- Strategic plans and business initiatives
- Employee records and personal information

Employees must ensure that confidential information is handled securely and disclosed only to authorized individuals who require the information for legitimate business purposes.

Employees must not:

- Share confidential information with unauthorized parties
- Store sensitive information on unsecured personal devices
- Discuss confidential matters in public spaces or unsecured communication channels
- Copy or remove sensitive data without authorization

Employees remain responsible for protecting confidential information even after their employment with Unosecur ends.

Any suspected data breach or unauthorized disclosure must be reported immediately to management or the Information Security team.

10. Cybersecurity Responsibilities

Because Unosecur operates in the technology and cybersecurity domain, all employees share responsibility for protecting the organization's digital infrastructure.

Cybersecurity is not limited to technical teams; every employee plays a role in maintaining a secure environment.

Employees must follow all established security practices and internal security policies.

Key responsibilities include:

- Using strong and unique passwords for company systems
- Enabling multi-factor authentication where required
- Avoiding the installation of unauthorized software
- Protecting laptops, mobile devices, and access credentials
- Following secure coding practices when developing software
- Reporting phishing attempts or suspicious digital activity

Employees must exercise caution when accessing company systems from remote environments or public networks.

Unauthorized access, misuse of systems, or negligent handling of security controls may result in disciplinary action and potential legal consequences.

Cybersecurity awareness training may be required periodically to ensure employees remain informed about emerging threats and best practices.

11. Responsible Use of Company Assets

Company resources are provided to employees for the purpose of performing their job responsibilities efficiently and effectively.

Company assets include but are not limited to:

- Computers, laptops, and mobile devices
- Software and licensed tools
- Cloud infrastructure and internal systems
- Office equipment and facilities
- Corporate communication systems
- Intellectual property and digital resources

Employees must use company assets responsibly and protect them from misuse, theft, or damage.

Employees must not:

- Use company systems for illegal activities
- Install unauthorized or pirated software
- Share login credentials with others
- Use company infrastructure for personal commercial purposes
- Circumvent established security controls

Limited personal use of company resources may be permitted if it does not interfere with work responsibilities, violate company policies, or expose the organization to security risks.

Managers may monitor usage of company systems in accordance with applicable laws and company policies.

12. Internet, Email, and Communication Systems

Company-provided communication platforms are intended for professional use and must be used responsibly.

These systems include:

- Corporate email accounts
- Messaging and collaboration tools
- Internal communication platforms
- Video conferencing systems
- Corporate documentation platforms

Employees must maintain professionalism and respect when communicating through these systems.

Employees must not use company communication tools to:

- Share offensive or inappropriate content
- Engage in harassment or discriminatory communication
- Distribute confidential information to unauthorized recipients
- Conduct illegal activities

Emails and messages sent using company systems may represent the organization and must be written clearly and professionally.

Employees should exercise caution when opening links or attachments from unknown sources to prevent cybersecurity threats.

The company reserves the right to monitor corporate communication systems in accordance with legal requirements and internal policies.

13. Social Media and Public Communication

Employees must exercise responsibility and professionalism when using social media or participating in public communication platforms.

While employees are free to express personal opinions in their private capacity, they must avoid presenting personal views as official statements of Unosecur.

Employees must not:

- Share confidential or proprietary company information
- Disclose customer data or internal discussions

- Post misleading or defamatory information about the company
- Represent the company publicly without authorization

Employees should be mindful that online activity may affect the reputation of the organization.

Any official communication on behalf of Unosecur must be authorized by management or designated communications personnel.

14. Intellectual Property Protection

Intellectual property developed within the scope of employment is a valuable asset of Unosecur and must be protected.

Intellectual property includes but is not limited to:

- Software source code
- Algorithms and security frameworks
- Product designs and architecture
- Documentation and research materials
- Proprietary tools or methodologies

All intellectual property created by employees during the course of their employment, using company resources or relating to company business, belongs to Unosecur.

Employees must not disclose proprietary information to external parties without authorization.

Employees must also respect the intellectual property rights of third parties and avoid unauthorized use of copyrighted materials, software, or confidential information belonging to others.

Violations of intellectual property protections may lead to disciplinary action and potential legal consequences.

15. Health and Safety

Unosecur is committed to maintaining a safe and healthy working environment for all employees.

Employees must follow established safety procedures and take reasonable precautions to prevent workplace accidents or injuries.

Employees are expected to:

- Maintain safe workspaces
- Follow emergency and evacuation procedures
- Report unsafe conditions immediately
- Use equipment responsibly

Employees should immediately notify management or Human Resources if they observe hazardous conditions or safety risks.

The company will take appropriate measures to investigate and address safety concerns.

16. Gifts, Hospitality, and Anti-Bribery

Employees must conduct business with honesty and integrity and must not engage in bribery, corruption, or unethical influence.

Employees must not offer, give, request, or accept anything of value that could improperly influence business decisions.

Acceptable business gifts must meet the following conditions:

- They are of nominal value
- They do not influence business judgment
- They are provided in a transparent and ethical manner

Examples of prohibited actions include:

- Accepting expensive gifts from vendors seeking favorable treatment
- Offering financial incentives to secure contracts or approvals
- Accepting payments or benefits in exchange for confidential information

Employees who receive gifts or hospitality that may create a potential conflict of interest must report them to management.

Unosecur maintains a strict zero-tolerance policy toward bribery and corruption.

17. Reporting Violations

Employees are encouraged and expected to report violations of this Code of Conduct or any suspected unethical behavior.

Reports may include concerns related to:

- Harassment or discrimination
- Fraud or corruption
- Misuse of company assets
- Security breaches or data leaks
- Legal or regulatory violations

Reports can be made through the following channels:

- Immediate supervisor or manager
- Human Resources Department
- Company leadership or designated compliance contact

Employees should provide as much factual information as possible when reporting a concern.

All reports will be treated confidentially and investigated appropriately.

Unosecur prohibits retaliation against any employee who raises a concern or reports a violation in good faith.

18. Investigation Procedures

When a report of misconduct or policy violation is received, the company will conduct a fair and impartial investigation.

The investigation process may include:

- Initial review of the reported concern
- Collection of relevant documentation or evidence
- Interviews with individuals involved or witnesses
- Evaluation of findings by management or Human Resources
- Determination of appropriate corrective actions

Investigations will be conducted in a confidential manner to protect the privacy of all individuals involved.

Employees are expected to cooperate fully with any investigation and provide accurate and truthful information.

Failure to cooperate or providing false information during an investigation may result in disciplinary action.

19. Disciplinary Actions

Violations of this Code of Conduct may result in disciplinary action depending on the nature and severity of the misconduct.

Possible disciplinary actions include:

- Verbal warning
- Written warning
- Mandatory training or corrective action plans
- Suspension of duties
- Termination of employment
- Legal action when applicable

Disciplinary decisions will be made after reviewing the facts of the situation and will be applied consistently and fairly.

Serious violations involving fraud, security breaches, harassment, or illegal activities may result in immediate termination.

20. Employee Responsibilities

All employees share responsibility for maintaining an ethical and professional workplace environment.

Employees are expected to:

- Read and understand this Code of Conduct
- Follow company policies and procedures
- Act with integrity and professionalism
- Protect confidential and sensitive information
- Report violations or concerns promptly
- Participate in required compliance or security training

Employees must seek guidance from management or Human Resources if they are uncertain about how to apply the principles outlined in this policy.

21. Policy Review and Updates

This Code of Conduct will be reviewed periodically to ensure that it remains aligned with organizational needs, regulatory requirements, and industry standards.

Updates may be made when necessary to address changes in laws, business practices, or company operations.

Employees will be notified when updates or revisions are issued.

The most current version of this policy will be maintained within the company's official policy repository.

22. Employee Acknowledgment

All employees are required to acknowledge that they have read, understood, and agree to comply with the provisions of this Code of Conduct.

Employee Name: _____

Employee Signature: _____

Date: _____

Manager Name: _____

Manager Signature: _____

Date: _____