GOVERNANCE & ETHICS

Code of Business Conduct & Ethics

The standards behind every connection.

Version 1.0

Effective: June 2026

Applies to all personnel, officers, directors, contractors, consultants, agents, and authorized representatives of CENTRA Digital Interconnect.

Table of Contents

1. A Letter from CENTRA Leadership

To our colleagues, customers, partners, suppliers, and the communities we serve,

CENTRA exists to accelerate digital services through secure, scalable, and neutral interconnection. The trust that carriers, cloud providers, enterprises, and partners place in us to support their critical infrastructure is our most valuable asset and our greatest responsibility.

This Code of Business Conduct and Ethics is our public covenant. It provides a transparent view into how we operate, how we make decisions, and what every individual and organization representing CENTRA is expected to deliver. These standards are non-negotiable. They allow us to serve as a neutral, trusted platform within a complex digital ecosystem, and they are the foundation on which we earn and maintain the confidence of every party we do business with.

Every person acting on behalf of CENTRA — whether employee, officer, director, contractor, consultant, agent, reseller, or representative — is personally responsible for understanding and upholding the standards set out in this Code. Where this Code requires a higher standard than commercial practice or local law, we adhere to the higher standard. Where this Code is silent, we default to integrity, transparency, and the long-term interests of those who rely on us.

We hold ourselves accountable to these principles, and we invite our customers, partners, and stakeholders to hold us accountable as well. Concerns can be raised through any of the channels described in this Code. Reports made in good faith are protected from retaliation without exception.

Thank you for the trust you place in CENTRA, and for the integrity you bring to every interaction on our behalf.

Approved electronically

Chris Machen

Chief Operating Officer (Top Management)
CENTRA

Approved electronically

Bryson Hopkins

VP of Security (Executive Sponsor)
CENTRA

2. Our Foundation: Purpose, Mission, and Trust

2.1 Who We Are

CENTRA operates secure, purpose-built interconnection facilities that enable carriers, cloud providers, content partners, and enterprises to exchange traffic and deliver digital services with confidence. We are a neutral platform: we do not compete with the customers who depend on us, and we do not favor one ecosystem participant over another.

2.2 Our Mission

Our mission is to accelerate digital services through a trusted, neutral interconnection platform that delivers secure, scalable, and low-latency connectivity at every facility we operate.

2.3 Why This Code Exists

Our business is built on trust. Customers entrust us with their critical infrastructure. Partners entrust us with shared commercial interests. Regulators entrust us with compliance. Communities entrust us with responsible operation of energy-intensive facilities. This Code formalizes the commitments we make to protect that trust in every interaction, in every market in which we operate.

Our Standard

Where this Code requires a higher standard than commercial practice or applicable law, we adhere to the higher standard. Where this Code is silent, we default to integrity, transparency, and the long-term interests of the parties who rely on us.

3. Scope: Who This Code Applies To

This Code applies to and is enforceable for:

1. All CENTRA employees, officers, and directors, regardless of role, level, location, or employment status (including full-time, part-time, temporary, and intern personnel);
2. Contractors, consultants, and temporary personnel performing work on CENTRA premises, on CENTRA systems, or on CENTRA's behalf;
3. Agents, resellers, channel partners, and representatives authorized to act on CENTRA's behalf;
4. Third party entities when acting or operating under the CENTRA name or brand; and
5. Any third party expressly required by contract to comply with this Code.

References in this Code to "CENTRA personnel," "you," or "individuals acting on CENTRA's behalf" should be read to include all of the above unless context indicates otherwise.

3.1 Personal Responsibility

Each individual covered by this Code is personally responsible for reading, understanding, and complying with it. Ignorance of the Code, of related CENTRA policies, or of applicable law is not a defense to a violation. Where a situation is not clearly addressed by this Code or where the right course of action is unclear, individuals are expected to seek guidance from their manager, the Legal & Compliance function, or through the reporting channels described in Section 30.

3.2 Supervisor Responsibility

Individuals who supervise others have an additional responsibility to model the standards of this Code, to foster an environment in which questions and concerns can be raised openly and without fear, and to take prompt and appropriate action when issues are reported. Supervisors must never retaliate against, ignore, or attempt to resolve outside of established channels any good-faith report of a potential violation.

4. Our Expectations of Partners, Suppliers, and Customers

CENTRA seeks to engage with organizations that share our commitment to ethical, lawful, and responsible business conduct. While this Code defines CENTRA's own standards, we expect our suppliers, vendors, channel partners, and customers to maintain their own equivalent commitments.

In particular, we expect our counterparties to:

1. Comply with all applicable laws and regulations in the jurisdictions in which they operate, including anti-bribery, sanctions, export controls, employment, privacy, and environmental laws;
2. Respect intellectual property rights and contractual obligations, both ours and those of third parties;
3. Protect shared, entrusted, and personal data using safeguards appropriate to its sensitivity and consistent with applicable law and recognized standards;
4. Maintain safe, lawful, and ethical workplaces, free from forced labor, child labor, human trafficking, and unlawful discrimination or harassment;
5. Operate honestly in commercial dealings, including pricing, billing, marketing claims, competitive practices, and the accuracy of information provided to CENTRA; and
6. Report concerns about CENTRA personnel, CENTRA-managed services, or business conducted under the CENTRA name through the channels set out in Section 30.

CENTRA reserves the right to evaluate the ethical and compliance practices of suppliers, partners, and other counterparties as part of due diligence, onboarding, and ongoing relationship management. Material or unresolved concerns may result in remediation requirements, suspension of activity, or termination of the relationship.

5. The CENTRA Framework: Five Guiding Principles

Our approach to ethical conduct is grounded in five principles. Every section that follows is an expression of one or more of these principles applied to a specific area of conduct.

INTEGRITY	We act honestly and transparently. Our communications, contracts, and commitments are clear, accurate, and reliable. We say what we mean and we deliver what we promise.
ACCOUNTABILITY	We own our decisions, our outcomes, and our mistakes. We measure success by the resilience of the infrastructure we operate and the trust of the ecosystem that depends on us.
SECURITY	Protecting data, networks, facilities, and partner information is foundational to our service — not an afterthought, not a feature, not an add-on. Every individual at CENTRA is a participant in our security posture.
NEUTRALITY	As a neutral interconnection provider, our platform's value depends on its impartiality. We engage with all ecosystem participants — carriers, cloud providers, enterprises, resellers, competitors of one another — fairly and without improper preference. We do not leverage our position to advantage or disadvantage any participant.
COMPLIANCE	We meet or exceed legal and regulatory requirements in every jurisdiction in which we operate, and we uphold high ethical standards even where the law is silent or ambiguous.

6. Compliance with Laws and Regulatory Frameworks

Compliance with the law is a baseline requirement at CENTRA. Legal obligations are not optional, situational, or subject to commercial pressure. Where legal or ethical expectations are unclear, CENTRA defaults to the highest applicable standard.

1. CENTRA complies with applicable local, state, federal, and international laws governing, without limitation:
2. Anti-bribery, anti-corruption, and anti-money-laundering;
3. Competition, fair dealing, antitrust, and consumer protection;
4. Data protection, confidentiality, and privacy (including, where applicable, U.S. state privacy laws.
5. Trade controls, economic sanctions, and export administration regulations;
6. Securities laws and the use of material non-public information;
7. Employment, labor, occupational health and safety, and human rights;
8. Environmental, building, fire, and energy regulations applicable to data center operations; and
9. Tax, financial reporting, and recordkeeping requirements.

Any attempt to evade legal or regulatory requirements — directly or through intermediaries, layered transactions, jurisdictional structuring, or other indirect means — is strictly prohibited and constitutes a serious violation of this Code.

Conflict Between This Code and Local Law

Where local law sets a higher standard than this Code, local law prevails. Where local law sets a lower standard, or is silent, this Code applies. Where compliance with this Code would require violation of a specific local law, individuals must promptly raise the conflict with Legal & Compliance before acting.

7. Anti-Bribery, Anti-Corruption, and Improper Payments

CENTRA maintains a zero-tolerance policy toward bribery, corruption, and improper influence, anywhere in the world. We compete on the merits of our platform, our operational performance, and the strength of our partnerships — never through favors granted in exchange for advantage.

7.1 Prohibited Conduct

No individual acting on CENTRA's behalf may, directly or indirectly:

1. Offer, promise, give, authorize, solicit, or accept any bribe, kickback, payoff, or improper advantage of any kind, whether monetary or in-kind;
2. Make or authorize a facilitation payment — a small payment to a government official to expedite a routine, non-discretionary action — even where local practice may treat such payments as customary;
3. Use a third party (such as an agent, consultant, distributor, or reseller) to make, conceal, or receive a payment that CENTRA itself would be prohibited from making or receiving;
4. Threaten, retaliate against, or pressure any colleague who refuses to participate in, or who reports, suspected bribery or corruption; or
5. Knowingly engage with a counterparty that is itself engaged in bribery or corruption in connection with CENTRA business.

7.2 Applicable Laws

This Code reflects, among other obligations, the requirements of the U.S. Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act 2010, and equivalent anti-corruption laws in other jurisdictions where CENTRA operates or where its counterparties are based. These laws apply broadly: they reach conduct of U.S. persons and companies anywhere in the world, conduct of any person within U.S. jurisdiction, and conduct that touches U.S. financial systems.

7.3 Dealings with Government Officials

Particular caution is required in any interaction with government officials, employees of state-owned or state-controlled entities, and members of their immediate families or households. Gifts, hospitality, travel, sponsorships, charitable donations, and offers of employment that involve such persons must be reviewed and pre-approved by Legal & Compliance in accordance with CENTRA's Anti-Bribery & Anti-Corruption Policy.

7.4 Due Diligence on Third Parties

CENTRA conducts risk-based due diligence on agents, consultants, and other third parties who interact with government officials or who may be perceived as acting on CENTRA's behalf. Engagements with such parties must be documented, justified, and supported by clear deliverables and reasonable compensation.

8. Trade Compliance, Sanctions, and Export Controls

CENTRA conducts its business in compliance with applicable trade laws, including economic sanctions, export controls, anti-boycott, and customs requirements imposed by the United States, the European Union, the United Kingdom, and other jurisdictions in which we or our counterparties operate.

8.1 Sanctions and Restricted Parties

CENTRA does not knowingly engage in transactions with individuals or entities that are subject to applicable sanctions, including parties listed on the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list, the EU Consolidated List, the U.K. Sanctions List, and equivalent restricted-party lists. Counterparties are screened on a risk-based basis as part of onboarding and on a periodic basis thereafter. Personnel who become aware that a CENTRA customer, supplier, or partner may be a restricted party — including through ownership or control by a restricted party — must promptly notify Legal & Compliance.

8.2 Embargoed Jurisdictions

CENTRA does not provide services to, or accept services from, jurisdictions subject to comprehensive U.S. embargoes, or otherwise engage in transactions prohibited by applicable trade laws. Activities involving jurisdictions subject to broad but not comprehensive sanctions require prior Legal & Compliance review.

8.3 Export Controls and Covered Telecommunications Equipment

Where applicable, CENTRA complies with export control regimes governing the transfer of regulated technology, software, and technical data. Where CENTRA is engaged in or supports U.S. federal government contracting, CENTRA complies with applicable Federal Acquisition Regulation (FAR) and Defense FAR Supplement (DFARS) requirements, including, where applicable, Section 889 of the John S. McCain National Defense Authorization Act, which restricts the use of certain covered telecommunications and video surveillance equipment in federal contracts.

8.4 Reporting Trade Concerns

Any concern about a potential sanctions exposure, restricted-party relationship, prohibited export, or unusual transaction structure must be raised with Legal & Compliance before the activity proceeds. Trade violations can result in severe civil and criminal penalties for both CENTRA and the individuals involved.

9. Conflicts of Interest

Individuals acting on CENTRA's behalf are expected to make decisions in CENTRA's interest, not in their own personal interest or the interest of a family member, friend, or other associated party. A conflict of interest exists when an individual's personal interests interfere — or could reasonably appear to interfere — with their objective judgment or duty to CENTRA.

9.1 Examples of Conflicts

Although the situations giving rise to a conflict are too varied to list exhaustively, common examples include:

1. Holding a material financial interest in a CENTRA customer, supplier, partner, or competitor;
2. Having a close family member or personal relationship with an employee of a CENTRA customer, supplier, partner, or competitor, where you are in a position to influence the relationship;
3. Serving as an officer, director, employee, consultant, or advisor of another organization that does business with, competes with, or seeks to do business with CENTRA;
4. Engaging in outside employment or business activity that materially interferes with CENTRA responsibilities or makes use of CENTRA confidential information, time, or resources;
5. Diverting a business opportunity that you become aware of through CENTRA to yourself or a related party;
6. Hiring, promoting, supervising, or evaluating a relative or close personal contact;
7. Accepting gifts, entertainment, loans, or other benefits in excess of what is permitted under Section 10 of this Code.

9.2 Disclosure and Management

Actual, potential, or apparent conflicts of interest must be disclosed promptly in writing to the individual's manager and to Legal & Compliance. CENTRA will work with the individual to determine an appropriate response, which may include declining to proceed with a transaction, reassigning responsibilities, removing the individual from a decision, implementing supervisory safeguards, or, where the conflict cannot be adequately managed, terminating the conflicting activity. Disclosure does not, by itself, resolve a conflict.

10. Gifts, Entertainment, and Business Courtesies

Modest, occasional gifts and business hospitality can help build legitimate working relationships. They must never be used — or appear to be used — to influence a business decision, secure an unfair advantage, or compromise the independent judgment of either CENTRA personnel or a counterparty.

10.1 General Standard

A gift, meal, or entertainment may be offered or accepted only if all of the following are true:

1. It is reasonable in value and not extravagant, judged by both U.S. and local norms;
2. It is infrequent, in good taste, and consistent with customary business practice;
3. It serves a legitimate business purpose and is not offered as, and could not reasonably be perceived as, a bribe, kickback, or reward for past or future business;
4. It does not violate any law, the policies of the recipient's organization, or any other CENTRA policy;
5. It is not in cash or a cash equivalent (such as gift cards, vouchers, or transferable credits);
6. It can be openly disclosed and accurately recorded in CENTRA's books and records.

10.2 Government Officials

Gifts, hospitality, travel, and entertainment offered to government officials or to employees of state-owned or state-controlled entities — regardless of value — require prior written approval from Legal & Compliance. Many jurisdictions impose strict limits or outright prohibitions on such offerings.

10.3 Reporting and Records

Gifts and entertainment given or received in connection with CENTRA business must be accurately reflected in expense reports and supporting records, including the purpose of the activity, the identity of the recipient or provider, and whether the counterparty is a government official or employee of a government entity.

11. Fair Competition and Market Conduct

CENTRA competes on the merits of its platform, operational performance, customer experience, and integrity of its partnerships. We comply with applicable competition, antitrust, and fair-dealing laws in every jurisdiction in which we operate, and we do not engage in anti-competitive conduct.

11.1 Prohibited Conduct

CENTRA personnel and authorized representatives may not, with competitors:

1. Agree on prices, fees, discounts, credit terms, or any other element of pricing;
2. Agree to allocate customers, markets, territories, or product or service lines;
3. Agree to limit production, supply, capacity, or output;
4. Agree to boycott or refuse to deal with any specific customer, supplier, or partner;
5. Coordinate responses to bids, tenders, or RFPs (bid-rigging); or
6. Exchange competitively sensitive information such as pricing, costs, margins, customer-specific terms, supplier terms, capacity plans, or strategic intentions.

11.2 Engaging with Competitors

Because CENTRA operates a neutral interconnection platform, some of our customers and partners are also competitors with one another or with us. Routine commercial and operational dealings with such parties are appropriate. However, particular care is required at industry events, standards, bodies, trade associations, and any forum where competitors are present. Discussions must be limited to legitimate, non-sensitive subjects; agendas should be set in advance; and personnel should withdraw from any conversation that moves into prohibited territory and report it to Legal & Compliance.

11.3 Fair Dealing with Customers, Suppliers, and the Public

All CENTRA personnel are expected to deal fairly with customers, suppliers, partners, competitors, and the public. Taking unfair advantage of another party through manipulation, concealment, misrepresentation of material facts, abuse of confidential information, or any other unfair-dealing practice is prohibited.

12. Use of Company Assets and Resources

CENTRA assets — including physical facilities, equipment, networks, systems, devices, funds, supplies, brand, information, and intellectual property — exist to support legitimate CENTRA business. Each individual covered by this Code is responsible for protecting these assets from theft, loss, damage, misuse, or waste, and for using them only for authorized purposes.

12.1 Physical Assets

Take reasonable precautions to prevent the theft, damage, or unauthorized use of CENTRA equipment and facilities. Report incidents of actual or suspected theft, damage, or misuse promptly to your manager and to Security.

12.2 Information Systems and Networks

CENTRA-issued devices, accounts, email, messaging platforms, and network access must be used in compliance with CENTRA's Acceptable Use Policy and Information Security Policy. Personal use must be incidental, lawful, and consistent with those policies.

12.3 Funds and Expenses

CENTRA funds, credit cards, and expense accounts must be used only for legitimate business purposes, properly approved and accurately documented.

12.4 Brand and Reputation

CENTRA's name, logo, marks, and reputation are valuable assets. Use of CENTRA branding outside of authorized business activity — including in personal social media, political activity, or third-party communications — is restricted and may require Marketing or Legal & Compliance approval.

13. Confidential Information and Intellectual Property

Confidential information is one of CENTRA's most important assets. It includes any non-public information relating to CENTRA, its customers, partners, suppliers, or employees that has commercial, operational, legal, or reputational value, provided in written or oral form, whether or not it is formally marked as confidential.

13.1 Examples of Confidential Information

Examples include, without limitation: customer identities, configurations, and traffic patterns; pricing, contract terms, and commercial strategy; network designs, capacity plans, and security architectures; financial information and forecasts; personnel information; business plans, M&A activity, and corporate transactions; technical specifications and proprietary methods; supplier and partner identities and terms; and any information received from a third party under an obligation of confidence.

13.2 Protecting Confidential Information

Individuals covered by this Code must:

1. Use confidential information only for the legitimate CENTRA business purpose for which it was provided;
2. Share confidential information only with persons who have a need to know and who are subject to a confidentiality obligation;
3. Apply safeguards appropriate to the sensitivity of the information. CENTRA workforce members (employees and contractors and consultants working on CENTRA systems) must apply safeguards consistent with CENTRA's Information Security Policy and data classification scheme. Vendors, partners, and other external parties must apply safeguards consistent with the security and confidentiality obligations in their agreement with CENTRA.
4. Avoid discussing confidential information in public places, on public networks, or in unsecured communications;
5. Avoid using non-approved messaging or file-sharing platforms for CENTRA business; and
6. Continue to protect confidential information after the engagement or employment relationship ends, in accordance with applicable agreements and law.

13.3 Intellectual Property

CENTRA respects the intellectual property rights of others and protects its own. Personnel must not knowingly infringe third-party copyrights, trademarks, patents, or trade secrets, and must not use, copy, or distribute third-party works (including software, written materials, or media) without appropriate authorization. Inventions, works, and improvements created in the course of CENTRA employment or engagement are governed by applicable agreements (including but not limited to employment, contractor, and assignment agreements).

14. Material Non-Public Information and Insider Dealing

In the course of CENTRA business, personnel may become aware of material non-public information ("MNPI") about CENTRA, its parent or affiliated entities, its customers, its partners, or its suppliers. MNPI is information that a reasonable investor would consider important in making a decision to buy, sell, or hold securities, and that has not been generally disclosed to the public.

14.1 Prohibited Conduct

Where any covered party (including a customer, partner, or supplier) is a publicly traded company, or its securities are otherwise tradable, personnel must not:

1. Trade in the securities of that party while in possession of MNPI obtained through CENTRA;
2. Disclose MNPI to family members, friends, or others outside of CENTRA, except as required for a legitimate business purpose and subject to appropriate confidentiality protections; or
3. Recommend ("tip") that another person trade in such securities based on MNPI.

14.2 CENTRA Itself

CENTRA, as of the effective date of this Code, is privately held. This section applies to MNPI concerning publicly traded customers, partners, suppliers, affiliates, or any future change in CENTRA's own status (for example, in connection with a financing, transaction, or public offering). All personnel must promptly raise any uncertainty about whether information constitutes MNPI with Legal & Compliance before acting on it.

15. Data Protection, Privacy, and Customer Data

CENTRA respects the privacy of individuals and protects personal data, Customer Data, and other sensitive information entrusted to us. We process personal data only for lawful, specified, and legitimate purposes, and we apply technical and organizational safeguards consistent with applicable privacy laws and recognized standards.

15.1 Customer Data

CENTRA personnel, contractors, agents, or representatives must not access customer equipment, except as expressly authorized by the customer or as required to deliver contracted services, to comply with law, or to respond to a security or safety incident. Customer Data is processed only in accordance with the applicable customer agreement and CENTRA's privacy notices and security commitments. “Customer Data” means information collected by CENTRA for the purpose of providing the services to Customer.

15.2 Personal Data

Personal data — information relating to an identified or identifiable individual — is collected, used, retained, and disclosed only in accordance with applicable law and CENTRA's Privacy Policy. Where required, CENTRA cooperates with customers and partners acting as data controllers to support their compliance obligations.

15.3 Cross-Border Transfers

CENTRA operates exclusively within the United States, and its facilities, systems, and personnel are located in the United States. Cross-border personal data transfers are not a routine feature of CENTRA’s operations.

15.4 Inquiries and Reporting

Privacy inquiries from individuals, customers, or regulators must be routed to Legal & Compliance promptly. Suspected or actual personal data incidents must be reported immediately in accordance with CENTRA's incident response procedures.

16. Information Security Responsibilities

Information security is a shared responsibility at CENTRA. Every individual covered by this Code participates in protecting the confidentiality, integrity, and availability of CENTRA systems, networks, facilities, and information.

16.1 Core Expectations

CENTRA Personnel are expected to:

1. Understand and comply with CENTRA's Information Security Policy, Acceptable Use Policy, and any role-specific security requirements;
2. Protect credentials, access tokens, and authentication devices, and never share them;
3. Use approved systems, applications, and channels for CENTRA business, and not use unapproved tools or shadow IT;
4. Apply appropriate handling and classification to information based on its sensitivity;
5. Complete required security awareness training and any role-specific security training;
6. Follow physical security requirements at CENTRA facilities, including badge use, visitor escort, and tailgating prevention; and
7. Promptly report suspected security incidents, vulnerabilities, lost or stolen devices, phishing attempts, and policy deviations through the channels described in CENTRA's incident response procedures.

16.2 Customer-Facing Trust Commitments

CENTRA is committed to establishing and maintaining a control environment aligned with recognized standards, including ISO/IEC 27001 and SOC 2, which CENTRA is actively pursuing. As CENTRA achieves and maintains these certifications and attestations, they represent commitments to customers and partners about how we operate. Personnel must support these commitments by following documented controls, contributing accurate and complete evidence to audit and assurance activities, and avoiding shortcuts that would compromise the integrity of the control environment

16.3 Responsible Use of Artificial Intelligence

CENTRA may use artificial intelligence (AI) tools — including generative AI assistants, large language models, and AI-enabled features within approved business applications — only in a manner consistent with this Code, the Acceptable Use Policy, the Information Security Policy, and applicable law.

CENTRA Personnel are expected to:

1. Use only AI tools that have been approved by CENTRA for business use; not introduce unauthorized or consumer-grade AI tools into CENTRA workflows;
2. Not input CENTRA confidential information, Customer Data, personal data, security-sensitive information, or any other non-public information into AI tools that have not been formally approved for handling that category of information;
3. Treat AI output as a draft or input, not as a final product — reviewing AI-generated content for accuracy, completeness, bias, and appropriateness before relying on it, sharing it, or incorporating it into CENTRA work product;
4. Disclose, where appropriate to the audience, that AI tools were used to generate or substantially shape a deliverable, particularly in customer-facing, regulatory, audit, or contractual contexts;
5. Respect intellectual property rights when using AI tools, including by not using AI to generate content that infringes third-party copyrights, trademarks, or trade secrets, and by complying with the licensing terms of any AI tool used; and
6. Not use AI tools to make consequential decisions about individuals (for example, hiring, discipline, access to services, or customer eligibility) without human review and accountability.
7. The list of approved AI tools, the categories of information that may be processed with each, and any role-specific restrictions are maintained by Information Security and Legal & Compliance and communicated through CENTRA's Acceptable Use Policy and related guidance. Questions about whether a particular AI use is permitted should be raised with Information Security or Legal & Compliance before the use occurs.

17. Accurate Recordkeeping and Financial Integrity

CENTRA's records are the foundation of accurate financial reporting, regulatory compliance, audit readiness, and informed business decisions. All CENTRA records — including accounting entries, invoices, expense reports, time records, contracts, Customer Data, operational logs, security records, audit evidence, and electronic communications — must be complete, accurate, and reliable in all material respects.

17.1 Prohibited Conduct

No undisclosed, off-the-books, or improperly recorded funds, assets, payments, or receipts may be created or maintained;

1. No record may be altered, falsified, concealed, or backdated. No records may be destroyed except in accordance with established CENTRA retention and disposal procedures;
2. No false or misleading entries may be made in any record, regardless of the apparent reason; and
3. No person may pressure, instruct, or induce another to do any of the above.

17.2 Retention and Holds

Records must be retained for the periods required by applicable law, contract, and CENTRA's records retention schedule. When a legal hold is issued — for example, in connection with litigation, an investigation, or a regulatory inquiry — the affected records must be preserved without alteration, and routine destruction must be suspended for the in-scope records until the hold is released by Legal & Compliance.

17.3 Cooperation with Auditors

Personnel must cooperate fully and honestly with internal and external auditors, regulators, and assessors. Withholding, misrepresenting, or obstructing access to information requested through a legitimate audit or investigation is a serious violation of this Code.

18. Communications, Monitoring, and Social Media

18.1 Approved Channels

CENTRA business must be conducted on approved CENTRA systems and applications. Personnel must not use personal email, personal devices outside of approved arrangements, or unapproved consumer messaging applications (including, by way of example, personal WhatsApp, Facebook Messenger, personal Signal accounts, or similar tools) to conduct CENTRA business, store CENTRA information, or communicate confidential information.

18.2 Monitoring of CENTRA Systems

CENTRA systems, devices, accounts, and networks are provided for legitimate business use. To the extent permitted by applicable law, and as documented in CENTRA's Acceptable Use Policy and applicable privacy notices, CENTRA may access, monitor, review, or disclose communications, data, and activity on CENTRA systems for purposes including security, compliance, investigation, legal hold, audit, and business continuity. Personnel should have no expectation of privacy with respect to CENTRA-managed systems beyond what is required by applicable law.

18.3 Speaking on Behalf of CENTRA

Only authorized spokespersons may speak on behalf of CENTRA to the press, analysts, investors, regulators, or the public. Requests for comment, interviews, speaking engagements, podcast appearances, and similar opportunities must be referred to Marketing or Legal & Compliance before a commitment is made.

18.4 Social Media

Personnel may engage on social media as private individuals, but must not imply that their personal views represent CENTRA, must not disclose CENTRA confidential information, and must not engage in conduct that would violate this Code if conducted in any other forum. CENTRA's separate Social Media Guidelines provide additional detail.

19. Respectful, Inclusive, and Harassment-Free Workplace

CENTRA is committed to maintaining a workplace built on dignity, mutual respect, and professional conduct. Discrimination, harassment, bullying, intimidation, and abusive behavior have no place at CENTRA, and are not tolerated.

19.1 Equal Opportunity

Employment decisions at CENTRA — including hiring, assignment, evaluation, promotion, compensation, training, discipline, and termination — are made on the basis of qualifications, performance, and business need. CENTRA prohibits discrimination on the basis of race, color, national origin, ancestry, religion, sex, gender, gender identity or expression, sexual orientation, age, disability, pregnancy, marital or family status, military or veteran status, genetic information, or any other characteristic protected by applicable law.

19.2 Harassment

Harassment — including unwelcome verbal, physical, visual, or written conduct that creates an intimidating, hostile, or offensive environment, or that is made a condition of employment or a basis for employment decisions — is prohibited. This includes, without limitation, sexual harassment, racial or ethnic harassment, harassment based on any protected characteristic, and retaliatory conduct.

19.3 Reporting

Anyone who experiences or witnesses discrimination, harassment, or other disrespectful conduct is encouraged to report it through the channels in Section 30. CENTRA will investigate reports promptly, fairly, and discreetly, and will take appropriate corrective action where a violation is substantiated. Retaliation against any individual who raises a good-faith concern is itself a serious violation of this Code.

20. Human Rights and Ethical Labor Practices

CENTRA respects the fundamental human rights of every individual affected by our operations, and supports internationally recognized human rights principles, including those reflected in the United Nations Guiding Principles on Business and Human Rights and the core conventions of the International Labour Organization.

CENTRA does not tolerate, and does not knowingly do business with parties that engage in:

1. Forced, bonded, indentured, or involuntary labor of any kind;
2. Child labor, as defined by applicable law and recognized international standards;
3. Human trafficking or any conduct that facilitates it;
4. Unsafe, unhealthy, or coercive working conditions; or
5. Suppression of lawful freedom of association or collective bargaining where recognized by local law.

CENTRA complies with applicable wage-and-hour, working-time, and labor protection laws, and expects its suppliers and partners to do the same. Concerns about human rights or labor practices — within CENTRA, within our supply chain, or among parties operating under the CENTRA name — should be raised through the channels in Section 30.

21. Health, Safety, and Well-Being

CENTRA operates power-intensive, mission-critical facilities where the safety of personnel, contractors, customers, and visitors is essential. We comply with applicable occupational health and safety laws and maintain practices designed to prevent injury, illness, and unsafe conditions.

21.1 Expectations

1. Follow all applicable health and safety requirements, procedures, and site rules at every CENTRA facility;
2. Use equipment, personal protective equipment, and facilities responsibly and as intended;
3. Promptly report unsafe conditions, near misses, incidents, injuries, and hazards;
4. Cooperate with safety drills, training, and incident investigations; and
5. Act in a manner that protects your own safety and the safety of others.

21.2 Substance Use

CENTRA maintains a workplace free from the impairing effects of drugs, alcohol, and other controlled substances. Personnel must not perform CENTRA work while impaired. Personnel struggling with substance use are encouraged to seek confidential support through available employee assistance resources before any policy violation occurs.

21.3 Violence and Threats

Threats of violence, acts of violence, intimidation, and weapons (other than lawfully carried tools necessary for permitted work) are prohibited at CENTRA facilities and in connection with CENTRA business.

21.4 Non-Retaliation for Safety Concerns

Personnel may raise safety concerns without fear of retaliation. Retaliation against any individual for raising a good-faith safety concern is a serious violation of this Code.

22. Environmental Responsibility and Sustainability

CENTRA recognizes that responsible environmental stewardship is essential to the long-term resilience of digital infrastructure and the communities in which we operate. CENTRA complies with applicable environmental laws and regulations and manages energy, water, refrigerants, fuel, and waste responsibly across its U.S. data center operations.

CENTRA is committed to:

1. Designing, building, and operating facilities to use energy and other resources efficiently;
2. Reducing environmental impact across facility operations over time;
3. Supporting environmentally responsible practices across our supply chain;
4. Cooperating with customers and partners on shared sustainability commitments; and
5. Continuously evaluating practical opportunities to improve environmental performance across our facilities.

Personnel and partners acting on CENTRA's behalf are expected to support these commitments through their day-to-day decisions, procurement choices, and operational practices.

23. Political Activities and Contributions

CENTRA respects the right of personnel to participate in the political process as private citizens, on their own time and using their own resources. CENTRA itself does not, however, make corporate political contributions to political parties, candidates, or campaigns except where expressly permitted by law and pre-approved by authorized executive leadership in accordance with this Code.

Personnel acting on CENTRA's behalf must not:

1. Use CENTRA funds, facilities, equipment, systems, time, or other resources to support personal political activity;
2. Imply, in personal political activity, that they speak for or represent CENTRA;
3. Pressure colleagues, subordinates, customers, suppliers, or partners to support a particular political position, candidate, or contribution; or
4. Make payments or in-kind contributions to officials or candidates with the intent or appearance of influencing CENTRA business.

Lobbying activity conducted on CENTRA's behalf — including engagement with regulators, legislators, and policy makers on issues that affect our business — must be authorized and conducted in accordance with applicable disclosure and registration laws.

24. Speaking Up: Reporting Concerns and Non-Retaliation

CENTRA's commitment to ethical conduct depends on people being willing to raise concerns. Anyone — employee, contractor, customer, partner, supplier, or member of the public — who suspects a violation of this Code, of CENTRA policy, of applicable law, or of any commitment CENTRA has made to its stakeholders is encouraged to speak up.

24.1 How to Raise a Concern

Concerns may be raised through any of the following channels:

1. Your direct manager or another member of leadership;
2. Human Resources, for personnel and workplace matters;
3. Legal & Compliance, for any matter under this Code;
4. Email: ethics@centradigital.com (monitored by Legal & Compliance);

24.2 Good-Faith Reporting

A report is made in good faith when the reporter honestly believes the information they are sharing may indicate a violation, even if it ultimately turns out to be unfounded. Good-faith reports are protected. Knowingly false, malicious, or retaliatory reports are themselves violations of this Code.

24.3 Non-Retaliation

CENTRA strictly prohibits retaliation against any person who, in good faith, raises a concern, reports a suspected violation, participates in an investigation, refuses to participate in conduct that would violate this Code, or exercises a legally protected right. Prohibited retaliation includes — without limitation — termination, demotion, reduction in compensation, exclusion, intimidation, harassment, negative reviews, and any other adverse action taken because of the report. Retaliation is a serious violation of this Code and is itself subject to discipline up to and including termination.

24.4 Confidentiality

CENTRA handles reports discreetly and limits disclosure to those with a need to know to investigate and respond. CENTRA cannot guarantee absolute confidentiality in every case — for example, where disclosure is required by law or by the requirements of a fair investigation — but it will protect reporter identity to the fullest extent practical.

25. Investigations and Due Process

Reports of suspected violations are taken seriously, evaluated promptly, and investigated fairly. CENTRA's investigation practices are designed to establish the facts, protect the individuals involved, preserve evidence, and arrive at a sound conclusion.

25.1 Investigation Standards

1. Initial assessment of a report is conducted within a reasonable period, typically five (5) business days of receipt;
2. Complex investigations are completed within thirty (30) calendar days of initial assessment, unless an extension is approved by Legal & Compliance;
3. Investigations document the allegation, evidence gathered, individuals interviewed, findings of fact, and recommended action;
4. Investigation records are retained securely for the period required by applicable law and CENTRA's retention schedule, and in any event for not less than five (5) years; and
5. Individuals involved in an investigation are expected to cooperate honestly and to refrain from discussing the investigation with others unless explicitly authorized by CENTRA Legal & Compliance.

25.2 Right to Respond

Any individual subject to a disciplinary investigation under this Code is informed of the substance of the allegation and given a reasonable opportunity to respond before a final disciplinary decision is made. The individual may provide a written statement, present relevant evidence, or identify witnesses with knowledge of the relevant facts. The response is considered before the final decision is reached. This section does not limit CENTRA's ability to take immediate protective action — such as suspending access — where necessary to protect systems, data, personnel, or the integrity of an investigation.

25.3 Outside Authorities

Nothing in this Code restricts any individual's legally protected right to report potential violations of law to a government agency or regulator, to participate in a government investigation, or to receive any monetary award offered by a whistleblower program. CENTRA does not require notice to the company as a condition of such reports.

26. Enforcement, Discipline, and Accountability

Violations of this Code may result in disciplinary action up to and including termination of employment or engagement, contract termination, recovery of compensation or benefits where permitted by law, legal action, and — where applicable — referral to law enforcement or regulatory authorities.

26.1 Factors Considered

CENTRA's response to a substantiated violation considers, among other things:

1. The severity, intent, and impact of the conduct;
2. Whether the individual self-reported and cooperated with the investigation;
3. Whether the conduct involved abuse of authority, supervisory failure, or retaliation;
4. Whether the conduct is a first offense or part of a pattern; and
5. Applicable law, contract terms, and prior CENTRA practice in comparable matters.

26.2 Categories of Personnel

Disciplinary outcomes vary by the category of personnel involved. For employees, outcomes may range from coaching to termination, consistent with applicable employment law. For contractors, consultants, and third parties, outcomes may include termination of the engagement or contractual remedies. For vendors and partners, outcomes are governed by the applicable agreement and CENTRA's Vendor Management Policy.

27. Acknowledgment and Training

27.1 Acknowledgment

All CENTRA personnel are required to acknowledge in writing that they have received, read, and agreed to comply with this Code:

1. Upon initial hire, engagement, or assignment to CENTRA;
2. Upon each material revision to this Code; and
3. Annually thereafter, on a schedule managed by Human Resources and Legal & Compliance.

Acknowledgments are recorded and retained as evidence of CENTRA's commitment to the standards in this Code.

27.2 Training

CENTRA personnel receive training on the topics covered by this Code on a regular basis, including at onboarding and at least annually thereafter. Additional role-specific training is provided where required by the nature of the role, applicable law, or contractual obligation. Completion of required training is mandatory.

28. Waivers and Exceptions

Any waiver of any provision of this Code must be approved in writing in advance, in accordance with the following:

1. For CENTRA personnel below the executive level: by Legal & Compliance, in consultation with the relevant function head;
2. For executives, directors, and officers: by CENTRA executive leadership or the body that holds equivalent governance authority, with appropriate disclosure where required by law or contract.

Waivers are granted only in limited circumstances where they are consistent with applicable law, the long-term interests of CENTRA, and the trust of the stakeholders this Code is designed to protect. No individual has authority to grant informal, retroactive, or implied waivers of this Code.

29. Governance and Review

This Code is owned by CENTRA executive leadership and is reviewed at least annually, and additionally upon any material change to CENTRA's scope, applicable laws, audit findings, or significant commitments to customers, partners, or regulators. The current version is the controlling version and supersedes all prior versions on its effective date.

30. Contact and Reporting Channels

Concerns, questions, and requests for guidance under this Code may be directed to:

LEGAL & COMPLIANCE	legal@centradigital.com
ETHICS & CONDUCT	ethics@centradigital.com (monitored by Legal & Compliance)
HUMAN RESOURCES	hr@centradigital.com
INFORMATION SECURITY	infosec@centradigital.com (for incidents, vulnerabilities, and security concerns)
PRIVACY	privacy@centradigital.com

A Note to Customers, Partners, and the Public

If you are not a CENTRA employee or contractor and you have a concern about CENTRA personnel, CENTRA-managed services, or business conducted under the CENTRA name, you are welcome to use any of the channels above. Reports made in good faith are treated discreetly and are not subject to retaliation.