

Duotech Services, LLC Privacy Program Plan

Duotech Services, LLC recognizes that information is a critical business asset. Protecting the confidentiality, integrity, and availability of our systems and data is fundamental to our operations, our customers, and the missions we support.

That responsibility extends to personal information.

We are committed to responsibly collecting, processing, storing, sharing, retaining, and protecting personal information entrusted to us by employees, applicants, customers, suppliers, contractors, business partners, website visitors, and other stakeholders.

The Duotech Services, LLC Privacy Program establishes a risk-based framework for managing personal information throughout its lifecycle. Our approach brings together privacy, cybersecurity, information security, legal and contractual requirements, risk management, business operations, and employee awareness.

1. Privacy Governance and Accountability

Purpose and Scope

The Duotech Services, LLC Privacy Program provides an organizational framework for managing privacy risk and protecting Personally Identifiable Information (PII), Personal Data, and other information subject to applicable privacy requirements.

The program is designed to:

- Establish accountability for privacy and data protection.
- Protect personal information from unauthorized or unlawful access, use, disclosure, alteration, loss, or destruction.
- Integrate privacy considerations into systems, technologies, projects, products, and business processes.
- Identify, assess, and manage privacy risks.
- Support applicable legal, regulatory, contractual, and customer requirements.
- Establish consistent practices for collecting, using, storing, transferring, retaining, and disposing of personal information.
- Provide appropriate transparency regarding our data practices.
- Promote a culture of privacy and cybersecurity awareness.

- Continually evaluate and improve our privacy safeguards.

The program applies to Duotech Services, LLC personnel, business operations, information systems, and third parties that process personal information on behalf of Duotech Services, LLC, as appropriate.

Privacy Leadership

Duotech Services, LLC designates appropriate personnel to oversee the Privacy Program and coordinate privacy activities across the organization.

Privacy oversight includes establishing policies, assessing risks, reviewing privacy practices, coordinating responses to privacy-related inquiries and incidents, and helping business functions understand their responsibilities.

Privacy is also a shared responsibility across the organization.

Key participants may include:

Senior Agency Official for Privacy — Appointed with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

Executive Leadership — Provides oversight, establishes organizational expectations, and supports appropriate resources for privacy and information protection.

Privacy, Legal and Compliance — Evaluates applicable requirements, maintains privacy policies and notices, supports individual privacy requests, and provides guidance concerning privacy obligations.

Cybersecurity and Information Technology — Establishes technical safeguards, identity and access controls, monitoring, vulnerability management, system security, and cybersecurity incident-response capabilities.

Human Resources — Manages privacy considerations associated with employees, applicants, contractors, benefits, payroll, training, and other workforce information.

Contracts and Program Management — Identifies privacy, cybersecurity, information-protection, and customer requirements associated with contracts and programs.

Supply Chain and Procurement — Evaluates appropriate privacy and security requirements for suppliers, subcontractors, service providers, and other third parties.

Employees and Contractors — Follow established privacy and information-security policies and promptly report suspected privacy or cybersecurity incidents.

2. Regulatory and Contractual Framework

Duotech Services, LLC evaluates the privacy and data-protection requirements applicable to its operations, contracts, customers, workforce, systems, and geographic locations.

Depending on applicability, these requirements may include federal and state privacy laws, international privacy requirements, government contracting obligations, customer requirements, and recognized information-security and privacy frameworks.

As a company operating within the defense industry, Duotech Services, LLC also recognizes the importance of coordinating privacy protections with cybersecurity requirements applicable to the Defense Industrial Base.

Our program may consider applicable requirements and guidance associated with:

- Personally Identifiable Information (PII)
- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)
- Defense Federal Acquisition Regulation Supplement (DFARS) requirements
- Cybersecurity Maturity Model Certification (CMMC) requirements
- NIST SP 800-171
- NIST SP 800-53
- NIST Privacy Framework
- Applicable U.S. state privacy laws
- Applicable international data-protection requirements
- Customer-specific privacy and security requirements
- Contractual data-protection obligations

Duotech Services, LLC periodically evaluates changes in applicable requirements and adjusts its policies, controls, and procedures as appropriate.

3. Information Lifecycle Management

Effective privacy management begins with understanding the information we collect, why we need it, where it resides, who can access it, and what happens to it throughout its lifecycle.

Data Inventory

Duotech Services, LLC seeks to maintain an appropriate inventory of personal information processed throughout the organization.

Depending on business requirements, this may include personal information relating to:

- Employees
- Job applicants
- Contractors
- Customers and customer representatives
- Government and industry partners
- Suppliers and subcontractors
- Business partners
- Website visitors
- Facility visitors
- Other individuals interacting with Duotech Services, LLC

Our inventory and recordkeeping processes are designed to help identify:

- Categories of personal information collected
- Categories of individuals associated with that information
- Sources of information
- Business purposes for processing
- Systems and locations where information is maintained
- Individuals and functions authorized to access the information
- Third parties receiving information
- Applicable retention requirements
- Security and privacy controls associated with the information

Data Flow Mapping

Where appropriate, Duotech Services, LLC maps how personal information moves through the organization.

This includes understanding how information:

Enters our environment through employment processes, websites, business applications, customer interactions, contracts, suppliers, physical facilities, and other authorized sources.

Moves among authorized systems, personnel, departments, and approved third parties.

Is processed for legitimate business, employment, contractual, security, compliance, or legal purposes.

Is stored within authorized systems and environments.

Is transferred or shared when required for legitimate and authorized purposes.

Is retained according to applicable business, contractual, legal, and records-management requirements.

Is securely disposed of when retention is no longer required.

Understanding these flows helps Duotech Services, LLC identify privacy risks and establish appropriate safeguards.

4. Data Minimization and Purpose Limitation

Duotech Services, LLC seeks to collect and process personal information only when reasonably necessary for legitimate business, contractual, employment, security, compliance, or legal purposes.

Where practical, our privacy practices are designed to:

- Define the purpose for collecting personal information.
- Limit collection to information appropriate for that purpose.
- Avoid unnecessary collection or duplication.
- Restrict processing to authorized purposes.
- Limit access according to role and legitimate business need.

- Establish appropriate retention periods.
- Securely dispose of information when it is no longer required.

Personal information should not be used for purposes that are incompatible with the reason it was collected unless such processing is otherwise authorized or permitted by applicable requirements.

5. Privacy Policies, Procedures and Notices

The Privacy Program is supported by internal policies, procedures, standards, and guidance designed to establish consistent expectations for protecting personal information.

These may address:

- Collection and use of personal information
- Data classification and handling
- Identity and access management
- Acceptable use of information systems
- Information sharing and transmission
- Records retention
- Secure disposal
- Remote access
- Physical security
- Third-party access
- Supplier and subcontractor requirements
- Privacy incident reporting
- Individual privacy requests
- Website and application privacy
- Cookies and similar technologies
- Cross-border data transfers, where applicable

Policies and procedures are periodically reviewed and updated based on changes in business operations, technology, risks, regulations, contracts, and customer requirements.

Privacy Notices and Transparency

Duotech Services, LLC seeks to provide appropriate notice regarding the collection and use of personal information.

Public-facing websites, portals, applications, and other services that collect personal information should provide appropriate privacy information based on the nature of the interaction and applicable requirements.

Where appropriate, privacy notices may describe:

- Categories of information collected
- Purposes for collecting information
- How information may be used
- Categories of recipients
- Retention practices
- Applicable individual privacy rights
- Cookies and similar technologies
- Methods for submitting privacy questions or requests

Duotech Services, LLC periodically reviews public-facing privacy notices and updates them when material data practices or applicable requirements change.

6. Privacy and Cybersecurity

Privacy and cybersecurity are closely connected.

Duotech Services, LLC employs administrative, technical, organizational, and physical safeguards designed to protect personal and sensitive information against unauthorized access, disclosure, alteration, loss, misuse, or destruction.

Our information-protection practices may include:

- Identity and access management
- Role-based or need-to-know access

- Authentication controls
- Network and endpoint security
- System monitoring
- Vulnerability management
- Secure configuration practices
- Encryption and other appropriate data-protection technologies
- Backup and recovery capabilities
- Physical security controls
- Incident detection and response
- Security assessments
- Personnel security practices

Security measures are selected based on factors such as the sensitivity of information, the nature and purpose of processing, applicable requirements, system architecture, and identified risks.

Access to personal information is restricted to authorized individuals with a legitimate business need and should be limited to the information necessary to perform their responsibilities.

7. Privacy by Design and Risk Assessment

Duotech Services, LLC seeks to integrate privacy considerations into the design, acquisition, implementation, and modification of technologies, systems, products, and business processes.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs), Data Protection Impact Assessments (DPIAs), or similar risk reviews may be conducted when a new or materially modified system, project, technology, vendor, or process involves significant processing of personal information.

Assessments may consider:

- Types and sensitivity of personal information

- Categories of affected individuals
- Purpose and necessity of processing
- Information sources
- Access requirements
- Information sharing
- Retention requirements
- Third-party processing
- Security controls
- Geographic location of processing
- Potential impact on individuals
- Legal, regulatory, contractual, and customer requirements

Identified privacy risks may result in additional safeguards, design changes, contractual controls, processing limitations, or other mitigation measures.

8. Individual Privacy Rights and Requests

Duotech Services, LLC recognizes that individuals may have certain rights regarding their personal information under applicable privacy laws.

Depending upon the applicable jurisdiction and circumstances, individuals may have rights to:

- Request access to certain personal information.
- Request correction of inaccurate information.
- Request deletion of certain information.
- Request restrictions on certain processing.
- Obtain information regarding how their data is used.
- Exercise other rights established by applicable privacy laws.

Duotech Services, LLC maintains procedures for receiving, evaluating, verifying, documenting, and responding to applicable privacy requests within required timeframes.

Where Duotech Services, LLC processes personal information on behalf of another organization, requests may be coordinated with that organization as appropriate.

9. Third-Party, Supplier and Subprocessor Management

Protecting information extends beyond Duotech Services, LLC systems and personnel.

Suppliers, subcontractors, consultants, cloud providers, technology companies, and other third-party service providers may process personal information while supporting our operations.

Duotech Services, LLC uses a risk-based approach to third-party privacy and cybersecurity management.

Depending upon the nature of the service and information involved, this may include:

- Privacy and cybersecurity due diligence
- Evaluation of security practices
- Contractual data-protection requirements
- Confidentiality obligations
- Restrictions on use and disclosure
- Access limitations
- Incident-reporting requirements
- Retention and disposal requirements
- Subcontractor or subprocessor requirements
- Appropriate flow-down of contractual obligations
- Periodic assessments or reviews

Third parties should process personal information only for authorized purposes and maintain safeguards appropriate to the sensitivity and risks associated with the information.

When a third party uses additional subprocessors, Duotech Services, LLC may require appropriate contractual and security protections based on applicable requirements and the associated risk.

10. Data Transfers

Personal information should only be transferred or disclosed for legitimate and authorized purposes.

Before transferring personal information to another organization or location, Duotech Services, LLC may evaluate:

- The purpose of the transfer
- Categories and sensitivity of information
- Recipient
- Destination
- Applicable contractual requirements
- Security of transmission
- Privacy and security practices of the recipient
- Applicable legal requirements

Where international transfers of personal information occur, Duotech Services, LLC evaluates applicable data-protection requirements and implements appropriate transfer mechanisms when required.

11. Data Retention and Secure Disposal

Personal information should not be retained indefinitely.

Duotech Services, LLC establishes retention practices based on business requirements, contractual obligations, legal requirements, security considerations, and records-management policies.

When information is no longer required, it should be securely deleted, destroyed, anonymized, or otherwise disposed of using methods appropriate to the sensitivity and format of the information.

Where a legal hold, regulatory requirement, contractual obligation, investigation, or other legitimate requirement applies, information may be retained for an appropriate additional period.

Duotech Services, LLC also expects applicable third-party processors to follow established retention and disposal requirements.

12. Privacy Incident and Breach Response

Duotech Services, LLC maintains processes for identifying, reporting, investigating, containing, and responding to suspected privacy and information-security incidents.

Employees and contractors are expected to promptly report suspected unauthorized access, disclosure, alteration, loss, misuse, destruction, or other potential compromise of personal or sensitive information.

Our response process may include:

Identification

Determine whether a privacy or information-security incident has occurred and identify the systems and information potentially affected.

Containment

Take appropriate action to prevent continued unauthorized activity, disclosure, or loss.

Investigation

Determine the nature, scope, cause, affected systems, information involved, and individuals or organizations potentially impacted.

Risk Assessment

Evaluate the sensitivity of affected information, potential consequences, contractual requirements, and applicable notification obligations.

Remediation

Address vulnerabilities, processes, configurations, procedures, or controls associated with the incident.

Notification

Provide notifications to affected customers, individuals, regulators, government organizations, contracting entities, or other appropriate parties when required by applicable law, regulation, contract, or customer requirement.

Lessons Learned

Review incidents to identify opportunities for strengthening controls, policies, procedures, training, and technologies.

Privacy and cybersecurity incidents are documented and tracked as appropriate to support accountability and continuous improvement.

13. Training and Privacy Awareness

Effective privacy protection depends on informed and responsible people.

Duotech Services, LLC promotes a privacy- and security-aware culture through policies, communications, guidance, and training.

Employees and applicable contractors may be required to complete periodic cybersecurity and privacy awareness training.

Training may include:

- Privacy fundamentals
- Personally Identifiable Information
- Data classification and handling
- CUI and FCI awareness, when applicable
- Phishing and social engineering
- Password and authentication security
- Secure information transmission
- Physical security
- Remote-work security
- Data retention and disposal
- Third-party information sharing
- Privacy incident identification and reporting

Personnel with specialized responsibilities or elevated access to sensitive information may receive additional role-based training.

14. Auditing, Monitoring and Program Effectiveness

Duotech Services, LLC periodically evaluates the effectiveness of its Privacy Program and supporting controls.

Privacy monitoring and assessment activities may include:

- Privacy policy reviews
- Data inventory validation
- Privacy risk assessments
- Access-control reviews
- Vendor and supplier assessments
- Security-control reviews
- Training completion monitoring
- Privacy incident trend analysis
- Records-retention reviews
- Internal assessments and audits
- Corrective-action tracking

Where assessments identify deficiencies or opportunities for improvement, corrective actions may be documented, assigned, prioritized according to risk, and tracked through completion.

15. Documentation and Recordkeeping

Duotech Services, LLC maintains appropriate records to support the operation and accountability of its Privacy Program.

Depending upon applicable requirements, documentation may include:

- Privacy policies and procedures
- Data inventories
- Data-flow documentation
- Privacy assessments

- Vendor assessments
- Data-processing agreements
- Privacy notices
- Training records
- Privacy requests
- Incident documentation
- Audit and assessment results
- Corrective actions
- Retention requirements

Documentation provides evidence that privacy risks are being identified, evaluated, and appropriately managed.

16. Continuous Improvement

Privacy is not a one-time compliance activity.

Privacy laws, cybersecurity threats, technology, business processes, government requirements, and customer expectations continue to evolve.

Duotech Services, LLC therefore periodically evaluates developments involving:

- Privacy and data-protection laws
- Defense-industry cybersecurity requirements
- Government contracting requirements
- Customer and contractual requirements
- Cybersecurity threats
- Emerging technologies
- Artificial intelligence
- Cloud technologies
- Business operations
- Supply-chain risks

- Data-processing practices

The results of these evaluations help guide improvements to policies, procedures, safeguards, technologies, training, and risk-management practices.

Our Privacy Principles

The Duotech Services, LLC Privacy Program is guided by a straightforward set of principles.

Accountability

We establish responsibility for protecting personal information throughout our organization.

Purpose

We collect and process personal information for legitimate and authorized purposes.

Minimization

We seek to collect and retain only the information reasonably necessary to fulfill those purposes.

Protection

We apply appropriate administrative, technical, organizational, and physical safeguards to information entrusted to us.

Access Control

We limit access to authorized individuals with a legitimate need for the information.

Transparency

We seek to provide appropriate information about how personal information is collected and used.

Risk Management

We identify, evaluate, and address privacy risks throughout the information lifecycle.

Third-Party Accountability

We expect suppliers, subcontractors, service providers, and other third parties entrusted with protected information to maintain appropriate safeguards.

Incident Preparedness

We maintain processes to identify, investigate, contain, remediate, and appropriately report privacy incidents.

Continuous Improvement

We periodically evaluate our Privacy Program and strengthen our practices as risks, technologies, regulations, and business requirements evolve.

Protecting Information Is Part of Our Mission

Customers, employees, partners, suppliers, and government organizations may entrust Duotech Services, LLC with important information.

Protecting that information is a responsibility we take seriously.

Our Privacy Program combines governance, responsible data practices, cybersecurity safeguards, risk management, employee awareness, supplier oversight, incident preparedness, and continuous improvement to protect personal information throughout its lifecycle.

We strive to collect only the information we need, use it appropriately, limit access, protect it from unauthorized activity, and securely dispose of it when it is no longer required.

For Duotech Services, LLC, protecting information is more than a compliance responsibility. It is an essential part of protecting our people, our customers, our business, and the missions we support.

Privacy Questions and Requests

Questions regarding the Duotech Services, LLC Privacy Program, the handling of personal information, or applicable privacy rights may be directed to:

Duotech Services, LLC

Privacy Contact: about@duotechservices.com

Address: 245 Industrial Park Rd, Franklin, NC, 28734 USA

Last updated: 2026-08-14