LEONARDO DRS

HOW WE SERVE

Code of Ethics and Business Conduct





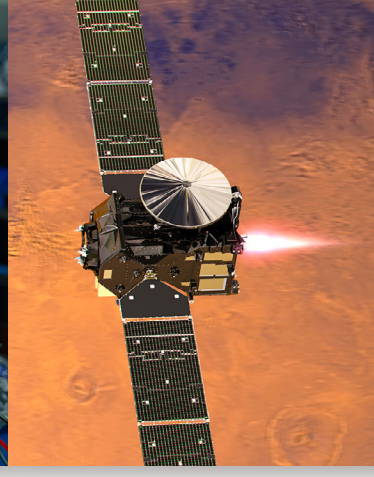



Table of Contents

A MESSAGE FROM OUR CEO 3

03 **HOW WE SERVE**

Our Commitment, Principles and Core Values 4
About This Code and Who It Applies To 5
Making Good Decisions and Living Our Values 6
Asking Questions and Speaking Up 7
Our Promise: No Retaliation 8

09 **COMMITMENT TO EACH OTHER**

Fostering Connectedness and Belonging 9
Respecting Equal Opportunity 10
Preventing Harassment and Bullying 11
Maintaining Health, Safety and Wellbeing 12

13 **COMMITMENT TO OUR COMPANY AND SHAREHOLDERS**

Protecting Company Assets 13
Using Technology and Artificial Intelligence (AI) Responsibly 14
Protecting Information and Data 15
Keeping Accurate Books and Records 16
Managing Records Properly 17
Avoiding Conflicts of Interest 18

19 **COMMITMENT TO OUR CUSTOMERS AND BUSINESS PARTNERS**

Producing Quality Products 19
Competing Fairly 20
Giving and Receiving Gifts Responsibly 21
Preventing Bribery and Corruption 22
Avoiding Insider Trading 23
Acting Ethically in Government Contracting 24
Handling Classified Information 25
Complying with Trade Laws 26
Preventing Money Laundering 27
Managing Third-Party Risks 28

29 **COMMITMENT TO COMMUNITY AND GLOBAL CONNECTION**

Respecting Human Rights 29
Protecting the Environment 30
Supporting Our Communities 31
Engaging in Political Activity Responsibly 32
Responding to Media and Government Inquiries 33
Using Social Media with Care 34

A Message from Our CEO

To my Leonardo DRS teammates,

Integrity, excellence and service are not just words for us at Leonardo DRS. They are the pillars of our identity. Our customers, partners and communities count on us to deliver advanced defense technologies, but more importantly, they trust us to do so with honesty, respect and accountability.

Our “We Serve” commitment reflects the reality that our primary customer is the military – and the stakes are measured in missions and lives. We serve by putting warfighter needs first, delivering on our commitments when it matters most, and treating every requirement, test and decision as a promise to those who depend on our work.

Now more than ever, we are asked to respond quickly to urgent customer needs. But urgency must never be an excuse to bypass or weaken our quality standards, commitments, legal obligations or core values.

This Code of Ethics and Business Conduct (the “Code”) is our shared guide. It reflects who we are: a company built on Integrity and Trust, Speed and Agility, Excellence, Customer Focus, Respect and Empowerment, and Innovation.

Our Code can help you face tough questions or situations that aren’t spelled out in a policy. If something feels wrong or confusing, speak up. Use your judgment. Ask for help. How we act, even behind the scenes, matters to our coworkers, with our customers and with our government partners.

Thank you for helping build a culture where doing the right thing is the only option.

Sincerely,

John Baylouny

John Baylouny
President & Chief Executive Officer
Leonardo DRS



How We Serve

Our Commitment, Principles and Core Values

Our values guide how we work, how we make decisions and how we treat one another.
They reflect who we are at Leonardo DRS (“DRS”) and what our customers, partners and communities expect from us.

These values shape how we live this Code.



INTEGRITY AND TRUST

We do what is right, even when no one is watching. We make decisions that reflect honesty, fairness and accountability.



SPEED AND AGILITY

We adapt quickly to changing needs and priorities. We deliver timely solutions that help our customers stay ahead.



EXCELLENCE

We hold ourselves to high standards and take pride in producing quality work. We learn, improve and strive to exceed expectations.



CUSTOMER FOCUS

We listen carefully, partner with our customers, deliver on our commitments and look for ways to add value. Our customers’ missions and success drive what we do.



RESPECT AND EMPOWERMENT

We foster a culture where everyone is treated with courtesy and professionalism. We give employees the tools, training and technology they need to work safely, speak up without fear of retaliation and contribute in meaningful ways.



INNOVATION

We invest in new ideas that advance technology, strengthen our capabilities and create better ways of working.

About This Code and Who It Applies To



This Code explains what DRS expects from everyone who works for or represents the company. It reflects our values and the responsibilities we all share.

The Code applies to:

- **All employees** of Leonardo DRS and its subsidiaries, including full-time, part-time and temporary workers
- **Leaders and governing bodies**, such as the board of directors, the CEO and officers
- **People and organizations acting for us**, including specifically consultants, agents, and sales representatives. They must agree in writing to follow the parts of the Code that apply to their work.

We expect everyone who represents DRS to follow the law, uphold our values and act with integrity.

Managers have added duties: set a strong example, explain expectations, listen to concerns, and make sure issues are handled or raised to the right place.

Our Expectations for Suppliers

We expect our suppliers and subcontractors to meet standards consistent with our own. This includes complying with laws and regulations applicable to their businesses, even when operating outside a home territory. Employees and managers who work with suppliers must use approved terms and conditions and ensure required obligations are flowed down.

Making Good Decisions and Living Our Values

This Code is your everyday guide to doing the right thing at DRS.
It brings our values to life and explains what is expected of each of us. You are not expected to know every law or policy by heart, but you are expected to pause, think and ask for help when something does not feel right.

An Ethical Decision-Making Model

When you face a tough decision, ask yourself:

Does it follow the law, contract terms and company policies?

- YES ✓ → **Is it consistent with our values and this Code?**
- NO OR UNSURE

Is it consistent with our values and this Code?

- YES ✓ → **Would you be comfortable if this issue became public?**
- NO OR UNSURE

Would you be comfortable if this issue became public?

- YES ✓ → **Does it respect the safety, dignity and rights of coworkers, customers and the public?**
- NO OR UNSURE

Does it respect the safety, dignity and rights of coworkers, customers and the public?

- YES ✓

If you answer “no” or feel unsure at any step,
stop 🛑 **and ask for help** from your manager, Human Resources, Legal or the Ethics and Business Conduct Office.



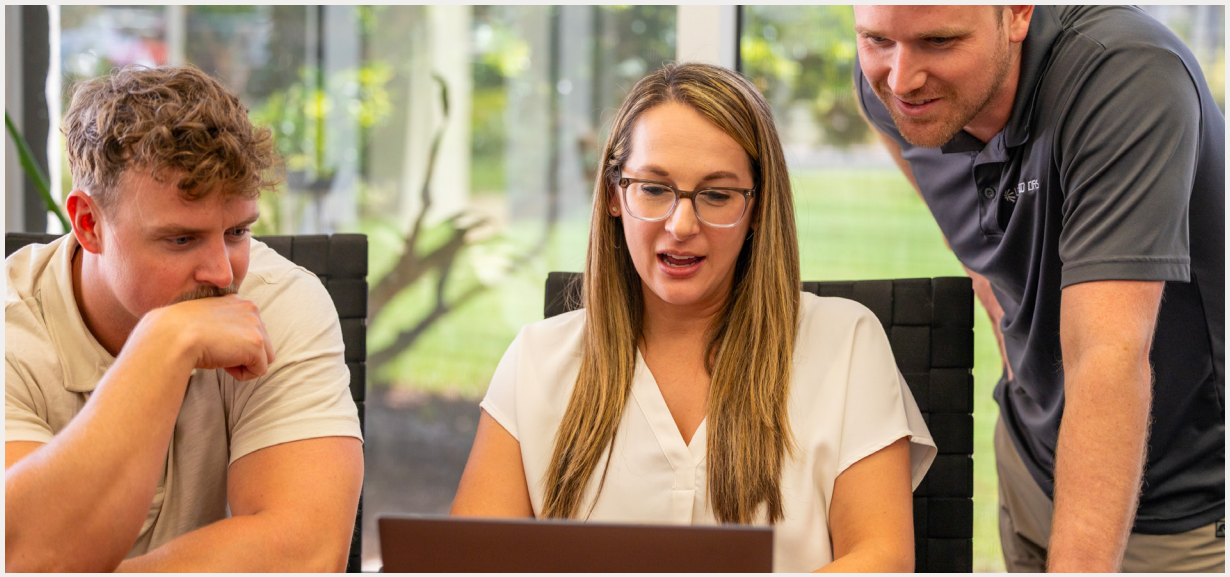
Certification and Training

- **Annual certification.** Each year, employees confirm in writing that they have reviewed the Code and will follow it. New employees complete this certification when they join DRS.
- **Ethics and compliance training.** Employees complete training regularly that explains the Code, highlights real-life situations and tests understanding.

If you are ever unsure about a requirement, or if you see someone ignoring the Code, speak up.

Asking Questions and Speaking Up

We strengthen DRS when we raise concerns early and ask for help when something does not seem right. Speaking up protects our people, our customers and our reputation. You are never expected to solve ethical issues alone, but you are expected to bring them forward.



Where to Go for Help

You can ask questions or report concerns through any of these channels:

- **Your supervisor or manager**
- **Human Resources**
- **A local Ethics Officer**
- **The Legal Department**
- **The Ethics and Business Conduct Office**
  by regular mail at:
  C/o Leonardo DRS, Inc. General Counsel
  Leonardo DRS Ethics and Business Conduct
  2345 Crystal Drive, Suite 1000
  Arlington, VA 22202
- **The DRS Alertline** – available 24/7 at **1-800-694-5005** or **https://drs.alertline.com**
  - Reports may be made anonymously.
  - After submitting, you will receive a PIN to check the status of your report.

All concerns are handled as confidentially as possible, and every report is reviewed and addressed in a timely manner.

Your Duty to Report

Every employee has a responsibility to speak up about possible misconduct, including violations of laws, regulations, company policy or this Code. If you see something wrong or are unsure whether something violates our standards, report it promptly. This includes concerns about:

- Fraud, theft or misuse of company assets including DRS intellectual property and controlled information
- Safety hazards or security risks
- Harassment or discrimination
- False claims, false statements or overpayments to the U.S. government
- Any action that conflicts with our values or obligations

If you are not sure whether something “counts,” report it anyway.

Cooperation in Investigations

DRS conducts fair and thorough investigations into reported concerns. Employees and consultants are expected to cooperate fully, provide truthful information and respond promptly to requests from investigators.

During an investigation:

- Share information only with the investigator or Legal Department.
- Do not discuss the matter with coworkers unless instructed.
- Do not hide information, mislead investigators or avoid interviews.

Failure to perform these actions can compromise the process and harm others.

If the investigation involves a government agency or outside authority, employees must coordinate their participation through the Legal Department.

Our Promise: No Retaliation

We want every employee to feel safe speaking up. DRS will not tolerate retaliation against anyone who raises a concern or takes part in an investigation in good faith.

Definitions

- **Retaliation** is any action meant to punish someone for asking a question, raising a concern or helping with an investigation. Examples include exclusion, unfair criticism, loss of opportunities, involuntary transfers or changes in treatment after speaking up.
- **Good faith** means you share what you believe to be true, even if an investigation later finds no violation.

Both engaging in retaliation and knowingly making a false or misleading report are serious Code violations, and either of them may lead to discipline or termination of employment or service contract.

Remember:

- **You are protected when you speak up.** No one may threaten, punish or treat you unfairly because you raised a concern or took part in an investigation.
- **You may refuse improper directives.** You will not be penalized for declining to follow instructions that break the law, violate policy or compromise the Code.
- **Report retaliation right away**. If you believe you or someone else is being retaliated against, contact your manager, HR, Legal or the Ethics and Business Conduct Office immediately.



Fostering Connectedness and Belonging

We Value Every Voice



DRS fosters a culture where every person feels seen, respected and empowered to contribute their unique perspective. We believe this drives innovation, strengthens teams and connects us to the communities we serve.

How We Promote Belonging

- **Value every voice.** Listen with respect and seek out differing opinions — especially from those whose experiences differ from your own.
- **Be a champion.** Speak up when you see or hear behavior that excludes or diminishes others.
- **Make space.** Ensure meetings, decisions and project opportunities include a range of perspectives.
- **Lead with empathy.** Treat colleagues with courtesy and respect across backgrounds, roles and locations.

Commitment in Action

Q: An employee wants to bring a dog to work for a health condition. What should I do?

A: Have them contact HR about a possible accommodation. Tell HR if you have safety or allergy concerns.

Q: An employee requests time and a private space for lactation.

A: Have them contact HR about a suitable accommodation.

Related Resources

DRS Employee Handbook

- HR1000 Equal Employment Opportunity and Affirmative Action
- HR1014 Disability Accommodation
- HR1026 Lactation Accommodation
- HR1032 Religious Accommodation
- HR1046 Animals in the Workplace
- HR5006 Reasonable Accommodations for Pregnant Workers

Respecting Equal Opportunity

We Uphold Respect for Every Person



Definitions

- **Equal opportunity:** Treating people fairly and making employment decisions based only on job-related factors
- **Protected characteristics:** Traits like race, color, religion, sex (including pregnancy), sexual orientation, gender, national origin, age, disability and veteran status, or any other status protected by applicable law

At DRS, we make employment decisions based on skills, effort and performance — not personal traits. Treating people fairly strengthens our teams and helps keep bias and discrimination out of decisions, from hiring to promotions.

How We Promote Fair Opportunity

- **Focus on merit.** Base your employment choices on qualifications, skills and results, not personal opinions or labels.
- **Watch for cognitive biases.** Notice patterns or comments in your own behavior and that of your teammates and say something
- **Be consistent.** Apply rules and expectations the same way for everyone.
- **Speak up.** Report concerns about discrimination or favoritism to HR, your manager or the DRS Alertline.

Commitment in Action

Q: During an interview, someone says an older applicant might not “fit in with our fast-paced team.” What should I do?

A: Speak up. Comments like that can indicate bias. Bring the focus back to skills and experience. Let HR know if you think this statement may lead to an unfair hiring decision.

Related Resources

DRS Employee Handbook

- HR1000 Equal Employment Opportunity and Affirmative Action
- HR1002 Harassment Prevention

Preventing Harassment and Bullying

We Treat Everyone with Dignity



Definitions

- **Harassment:** Unwelcome speech, imagery, physical or electronic conduct tied to a protected trait that creates a hostile, intimidating, degrading or offensive environment, and unreasonably interferes with an employee's work performance
- **Sexual harassment:** Unwelcome sexual advances, requests or conduct of a sexual nature that interferes with an employee's work performance, creates a hostile environment or is tied to employment decisions
- **Bullying:** Repeated, inappropriate behavior — including threats, humiliation or sabotage — that undermines someone's dignity or work, even if not based on a protected trait

Harassment and bullying have no place at DRS. We expect a professional, respectful atmosphere — in our facilities, at customer sites and anyplace where we work or represent the company. Everyone should feel safe to speak up and do their best work.

How We Prevent Harassment and Bullying

- **Set the tone.** Be courteous in words, images and actions — online and in person.
- **Speak up.** If you see or experience harassment, report it to a manager, HR or the DRS Alertline. Retaliation is not allowed.
- **Respect boundaries.** Do not share unwanted messages or images or engage in unwanted touching.
- **Lead fairly.** Apply rules and feedback consistently. Do not tolerate bullying, intimidation or exclusion.
- **Know the policy.** Follow our Harassment Prevention policy wherever work happens — on-site, off-site and at events.

Commitment in Action

Q: A manager keeps "joking" about an employee's accent in meetings. People laugh, but the team member looks uncomfortable. What should I do?

A: Say something and report it. Comments about someone's background can be harassment or bullying, even if called a joke. Support the team member, flag the issue to the manager to stop the behavior and contact HR or the DRS Alertline so we can address it.

Related Resources

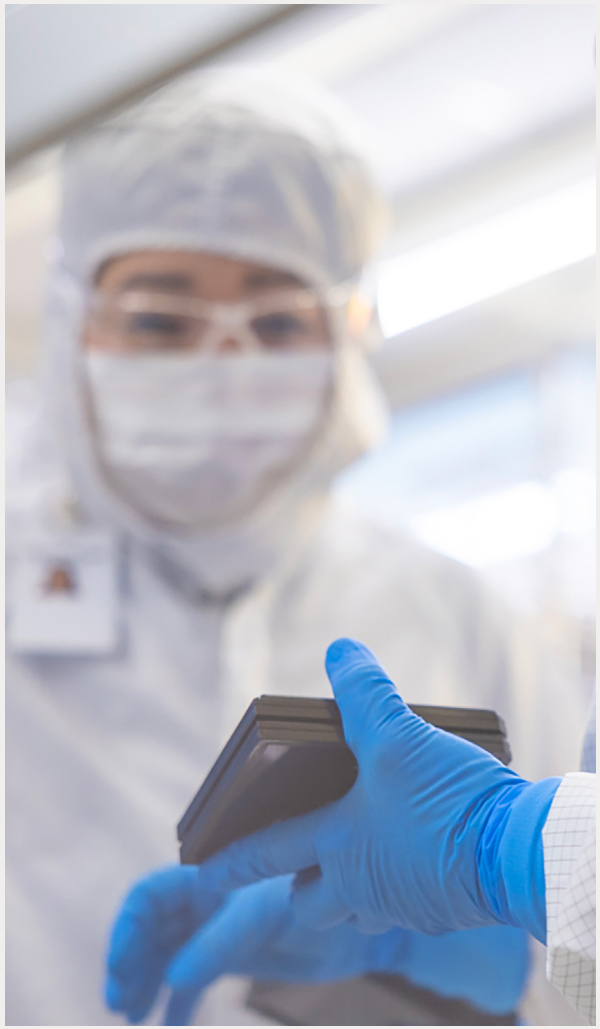
DRS Employee Handbook

- HR1002 Harassment Prevention

Maintaining Health, Safety and Wellbeing

We Protect Ourselves and Each Other

DRS is committed to a safe, healthy and supportive workplace. We strive to prevent harm by adopting and following safety rules, watching out for one another and speaking up early when something feels unsafe or unhealthy. Supporting wellbeing helps us think clearly, stay safe and do our best work.



How We Serve

- **Work safely.** Follow all rules, procedures and training for your role, including wearing any required personal protective equipment. Stop work if conditions are unsafe.
- **Report hazards and concerns.** Tell a manager, an Environmental, Health & Safety (EH&S) coordinator or Security right away if you see a spill, hazard, injury or health concern — even a minor one.
- **Prevent violence.** Never threaten, intimidate or harm anyone. Report concerning behavior immediately.
- **Do not bring weapons.** Weapons are not allowed on company property or at company events unless required for the job.
- **Control access.** Follow visitor, badge and escort procedures. Report strangers in secure areas.
- **Use leave when needed.** Health & Emergency Leave is available for illnesses, medical appointments, family care needs and emergencies.
- **Stay substance-safe at work.** Do not work under the influence of illegal drugs, medications or alcohol. If a medicine could affect your ability to work safely, tell your manager and HR.
- **Know the signs.** If you or a coworker seems unusually stressed, fatigued or distracted, check in or alert a manager.
- **Ask for help.** The Employee Assistance Program offers 24/7 confidential support for personal, family, financial or emotional challenges.

Handling a Crisis at Work

- Protect yourself first by moving to a safe place and following the directions of emergency responders, Security or EH&S.
- Call 911 in life-threatening emergencies, then notify your manager, Security or EH&S when it is safe.
- Stay calm, use evacuation routes or shelter areas and check in when directed.
- Report what you saw afterwards so hazards or injuries can be addressed.

Commitment in Action

Q: A contractor is not wearing required eye protection in a test area. Should I say something?

A: Yes. Safety is everyone's responsibility. Remind them or alert your manager or EH&S. Acting quickly prevents accidents.

Related Resources

DRS Employee Handbook
- HR1004 Substance Abuse Prevention
- HR4020 Health & Emergency Leave
- HR5004 Employee Assistance Program
- HR6002 Health and Safety

EHS-001 Environmental Health and Safety Policy
SEC-003 Visitor Control Policy
SEC-006 Workplace Violence Policy
SEC-007 Weapons in the Workplace Policy

Protecting Company Assets

We Safeguard What Powers Our Mission

Our work depends on the tools, systems and information we use every day. Caring for these assets shows respect for each other's work and for the people who trust us with sensitive information.

Misusing or losing company assets can delay work, put people at risk, violate laws or harm our reputation. Protecting them keeps programs on track, supports national security and strengthens performance.

How We Protect Company Assets

- **Use assets for business.** Use company tools, systems and facilities for work. Do not allow any use that could affect safety, security, compliance, productivity or performance.
- **Secure physical property.** Take care of equipment, badges and keys. Lock work areas, store sensitive items properly and report loss, theft or damage right away.
- **Protect information.** Treat confidential information, including Company Controlled Information (CCI), trade secrets, other intellectual property, technical data and Personally Identifiable Information (PII), as need-to-know and in accordance with DRS policy and legal requirements.
- **Follow cyber and IT rules.** Use IT assets and IT services in accordance with our policies. Do not transfer company information, including CCI, to unauthorized, non-DRS IT assets or IT services such as personal email, cloud storage or removable media.
- **Manage visitors carefully.** Follow sign-in, badging and escort procedures. Do not let visitors enter sensitive areas or see protected information unless approved.
- **Practice maintaining a clean workspace.** Keep desks, conference rooms and shared areas free of unattended documents and devices. Secure these spaces when you leave.

Definition

- **Company Controlled Information (CCI):** Unclassified company or program information that must be safeguarded, such as trade secrets, controlled government unclassified information, export-controlled data, technical data, personal information and other protected information.



Commitment in Action

Q: I sometimes email work files to my personal email to catch up at home. Is that okay?

A: No. Company information is authorized for use and access only on DRS IT assets and IT services. Using personal email or devices increases the risk of loss or misuse and may violate laws or contracts. Contact IT for assistance with working or printing from home.

Related Resources

DRS Employee Handbook
- HR1040 Visitors in the Workplace
- HR1042 Workplace Conduct

CITG-001 Cyber / IT Acceptable Use Policy
LEG-005 Intellectual Property and the Protection of Proprietary Information
SEC-003 Visitor Control Policy

Using Technology and AI Responsibly

We Protect Data and Use Tools Wisely

Technology helps us work efficiently, but it carries risks. In the face of cyber threats and potential data theft, we must use company systems and approved AI tools in ways that protect DRS, our customers and our information.



How We Serve

- **Use company systems for business.** Use company IT assets for DRS work. Do not bypass security tools or install unapproved software.
- **Protect Company Controlled Information (CCI).** Store and share it only through approved systems. Follow need-to-know rules for digital and paper records.
- **Work securely when remote.** Use the VPN as required, protect your screen and keep company devices under your control. Do not let others use your work devices.
- **Use AI tools carefully.** Use only approved Generative AI tools. Never paste CCI, including export-controlled data, customer data or personal data, into public or unapproved AI tools.
- **Verify AI output.** Treat AI-generated content as a draft. Check it for accuracy, bias and intellectual property concerns before using it.
- **Report issues immediately.** Report suspected cyber incidents, lost devices, data mishandling or risky generative AI use, for example, uploading sensitive company financial reports into a public tool, to IT, Cybersecurity or the DRS Alertline.

Definition

- **Artificial intelligence (AI):** Technology that uses data and algorithms to perform tasks that normally require human judgment, such as recognizing patterns or making suggestions. “Generative AI” is a type of AI that creates new content — like text, images, code, audio or video — in response to prompts.

Secure Remote Work

- Use approved DRS IT assets and IT services when handling CCI.
- Keep company devices under your control and do not let others use them.
- Protect your screen contents and be aware of who can see or hear your work.
- Store printed materials safely and shred them when they are no longer needed.

Commitment in Action

Q: Can I paste text from a customer Statement of Work into a public AI tool?

A: No. Never enter CCI into unapproved AI tools.

Q: Can I paste text from a partner or supplier quote or proposal into a public AI tool?

A: No. Never enter CCI into unapproved AI tools. Use approved tools or draft the response yourself and ask the data governor or Legal if you’re unsure about the output.

Related Resources

CITG-001 Cyber / IT Acceptable Use Policy
CITG-002 Program Data Governance Policy
LEG-009 Generative Artificial Intelligence Policy

Protecting Information and Data

We Safeguard What Powers Our Work

DRS relies on designs, data, know-how and personal information to operate, support our customers and meet legal and contractual obligations. We must protect this information, use it only for valid business purposes and follow all rules for sharing, storing and securing it.

How We Serve

- **Protect sensitive information.** Handle CCI, including confidential information, trade secrets and other intellectual property, technical data and Personally Identifiable Information (PII) with care. Share it only in accordance with DRS policy and legal requirements and only with authorized people who need it to do their work.
- **Use the right agreements.** Before sharing DRS information outside the company, confirm that a Non-Disclosure Agreement (NDA) or another approved contract is in place. Ensure the information is marked appropriately. Share only what is needed and follow the limits in the agreement.
- **Store and handle information correctly.** Use required markings and keep CCI only in approved IT systems or secure locations. Do not move CCI to any unauthorized, non-DRS IT assets, personal email, cloud storage or removable media.
- **Respect intellectual property and data rights.** Follow rules for inventions, patents, copyrighted works, trademarks and trade secrets. Do not use or share another organization's protected information without written permission.
- **Protect personal information.** Treat employee and other personal data as confidential. Access, update or share it only if your job requires it and you are authorized. Send outside requests for employment or pay information to Human Resources.
- **Control access to regulated data.** Follow DRS policies including the Technology Control Plan, Electronic Communications Plan and Visitor Control Policy. Do not allow access to export-controlled or other regulated data unless a license, exemption or written approval allows it.
- **Discuss sensitive topics in safe spaces.** Do not talk about sensitive information in public areas, on unsecured calls, on speakerphone or through personal apps. Protect what is on your screen.
- **Report issues right away.** If information or personal data is lost, mishandled or accessed improperly, contact Security, Legal, Cybersecurity or your manager immediately.

Information Requiring Extra Care

- Export-controlled data and software must stay in approved systems and may not be shared with foreign persons unless authorized.
- Invention disclosures help DRS protect new ideas and meet contract requirements.
- Customer-furnished information must be used only as instructed in the contract or written guidance.

Commitment in Action

Q: I need to send drawings to a supplier and respond to a request for employment information. What should I do?

A: Confirm an NDA is in place before sharing drawings and check whether they contain regulated data. Use approved tools and share only what is necessary. Ensure the information is marked appropriately. Send employment-related requests to Human Resources.

Definition

- **Personally Identifiable Information (PII):** Personal information that can identify someone, such as a name with an address, a Social Security number or a birth date

Related Resources

LEG-005 Intellectual Property and Proprietary Information
SEC-002 Technology Control Plan
SEC-003 Visitor Control Policy
DRS Employee Handbook
- HR-2000 Access to Employee Records

CITG-001 Cyber / IT Acceptable Use Policy
CITG-002 Program Data Governance Policy

Keeping Accurate Books and Records

We Tell the Full, True Story of Our Business

Accurate records help us make good decisions and keep trust with customers, shareholders and regulators. Because much of our work involves government contracts, mistakes in our books can create serious legal and financial risk.

How We Serve

- **Record transactions fully and on time.** Capture time, costs, revenues, test results and other data as work happens. Do not "recreate" the week or month later.
- **Follow approved processes and systems.** Use only authorized tools for timekeeping, expenses, purchasing, invoicing and reporting. Do not keep unapproved logs or spreadsheets as the record of work.
- **Use the right charge numbers.** Charge time and costs to the correct project or cost objective. Never move hours or costs to meet a target or "use up funding."
- **Support estimates with facts.** Base bids and cost estimates on current and accurate data, and share updates if new facts change the numbers.
- **Retain records as required.** Keep contracts, invoices, test data, timecards and other records according to the Records Retention policy, including the schedule of when to retain or destroy documents. In the event of an audit, investigation or legal hold, do not follow the normal destruction schedule and await instruction from Legal instead.
- **Do not allow false entries.** Never create, change or sign a record if it is incomplete, misleading or false. Speak up if you see altered documents, missing approvals or unrecorded cash, assets or liabilities.
- **Ask questions and report concerns.** If unsure how to record something, ask Finance, Legal or your manager. Report suspected false claims, inaccurate records or mischarging right away.

Definition

- **Books and records:** Documents that show our business activities, such as timecards, contracts, invoices, test reports and financial statements



Commitment in Action

Q: My manager asked me to move hours to a contract to recover more costs. What should I do?

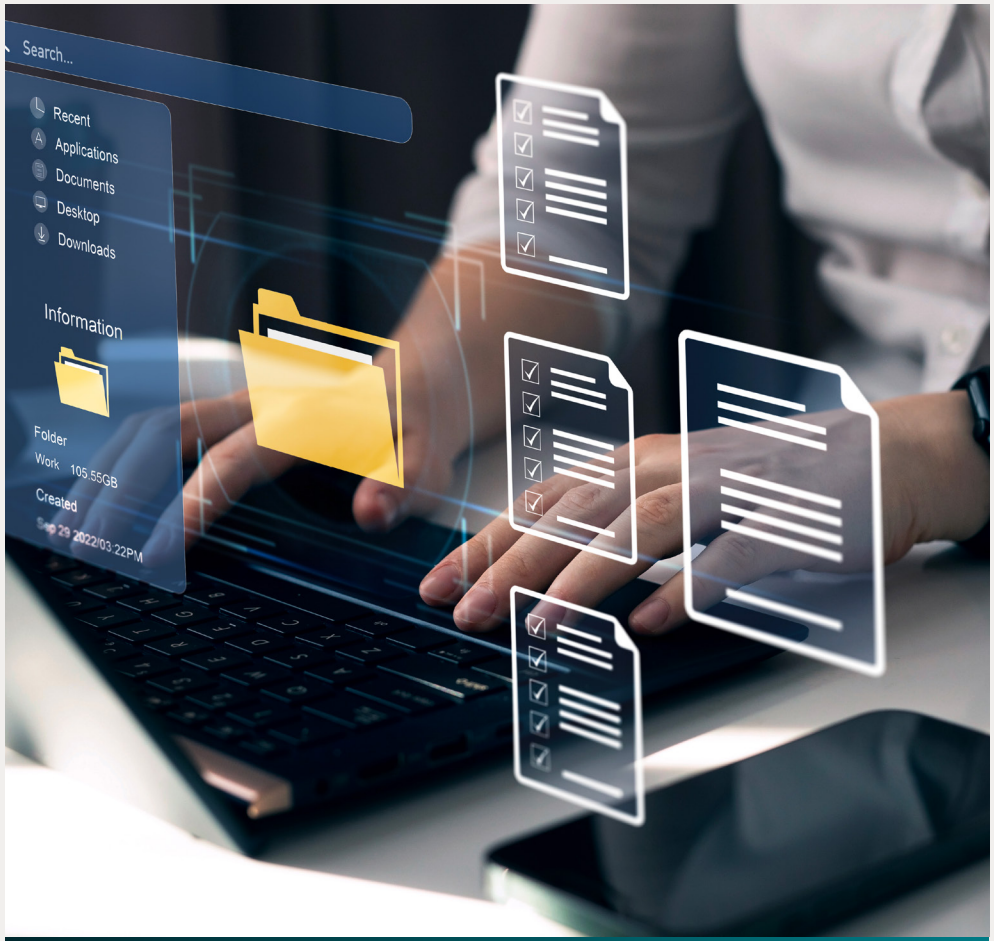
A: Do not change records to meet a budget. Charge time to the work actually performed and report pressure to Finance, Legal or the DRS Alertline.

Related Resources

CON-003 Using Cost or Pricing Data for Definitizing a Negotiated Procurement
CON-100 Records Retention
FIN-16.4 Labor Charging

Managing Records Properly

We Retain and Dispose of Records the Right Way



DRS keeps records to run the business and meet legal, contract and tax obligations. Managing them correctly helps us stay organized and ready for audits, reviews or investigations.

How We Serve

- **Follow the Records Retention policy.** Keep and dispose of records according to the Records Retention Schedule. If a law, contract or customer requires more time, follow that requirement.
- **Honor legal holds.** Never destroy or change records under a legal hold or preservation notice. When in doubt, keep the record and check with Legal.
- **Review before destruction.** Before disposing of records, confirm there is no legal, customer or business reason to keep them. Do not destroy records tied to a dispute or audit without guidance.
- **Treat electronic data as records.** Manage emails, shared folders and program data the same way as if they were printed on paper. If it meets the definition of a record, retain or delete it according to policy.
- **Do not keep records longer than needed.** Destroy drafts and old working files when they are no longer useful and not under a hold. Use approved disposal methods.
- **Ask when unsure.** If you do not know whether something is a record or how long to keep it, ask your manager, records coordinator, program data owner or Legal.

Commitment in Action

Q: Our files are past their retention date, but they may be relevant in a lawsuit. What should I do?

A: Do not destroy or alter anything. Check with Legal and wait for clear instructions.

Definitions

- **Retention period:** Required time a record must be kept
- **Legal hold:** A notice to stop destruction because of litigation or investigation

Related Resources

CON-100 Records Retention
CITG-002 Program Data Governance Policy

Avoiding Conflicts of Interest

We Put DRS Interests First

A conflict of interest happens when personal interests or relationships could affect — or appear to affect — how we act for DRS. We must make business decisions based on what is best for DRS, not on personal gain, outside work or family ties.



When in Doubt, Disclose

Conflicts often involve perception.

- A situation can still be a concern even if you believe you can stay objective.
- Many conflicts can be managed and/or mitigated if raised early.
- The failure to disclose is often more serious than the conflict itself.

If unsure, treat the situation as a potential conflict and ask for guidance.

How We Serve

- **Avoid situations where relationships affect judgment.**
  - Do ***not*** take part in decisions involving a family member, close friend or anyone whose interests could influence your choices.
  - Do ***not*** hire, supervise or make business decisions about a family member or close personal relation without review and written approval.
- **Disclose early.** If something could be or even look like a conflict, report it through the personal conflict of interest (PCOI) process before you act and wait for guidance.
- **Use the PCOI process for outside work or employment.** Get approval before taking outside jobs, consulting work or board roles that could overlap with DRS interests or time commitments.
- **Watch financial interests.** Avoid significant financial interests in companies that compete or do business with DRS unless approved.
- **Use DRS property only for DRS business.** Do not use the DRS name, information or resources for personal projects or gain.
- **Raise related-party issues.** If directors, officers, significant shareholders or their immediate family members, including spouses, children, siblings and parents, may benefit from a DRS transaction, notify the general counsel.
- **Ask when unsure.** If you are not sure whether something is a conflict or how to manage it, ask your manager, Ethics and Business Conduct or Legal.

Definitions

- **Personal conflict of interest (PCOI):** When personal interests may interfere — or appear to interfere — with acting objectively for DRS
- **Close personal relation:** A family member or someone with a close bond whose relationship could affect work decisions
- **Financial interest:** A stake in another company that could create personal gain or loss
- **Related party:** Certain leaders, significant shareholders and their immediate family members, including spouses, children, siblings and parents, whose dealings with DRS need review

Commitment in Action

Q: My sister works for a key DRS supplier, and I help evaluate that supplier. Do I need to say anything?

A: Yes. Disclose the situation through the PCOI process and pause your involvement until you receive guidance.

Related Resources

EBC-002 Personal Conflicts of Interest
EBC-010 Related Party Transactions
CON-015 Organizational Conflicts of Interest

Producing Quality Products

We Build What We Promise

DRS earns customer trust by delivering products that meet requirements and perform as promised. Quality depends on each of us, from design through production, testing and support. Meeting contract, safety and quality requirements protects our customers, our reputation and our future business.



Definitions

- **Product substitution:** Delivering items that do not meet requirements, using unapproved parts or processes or skipping tests
- **Nonconforming material:** Anything that does not meet drawings, specifications, contract terms or approved changes
- **Traveler/build record:** The document or system record showing each required step, inspection and test for a product

How We Serve

- **Know and follow requirements.** Understand the drawings, specifications, work instructions and quality procedures for your job. Ask questions before you start if anything is unclear.
- **Complete required inspections and tests.** Do not skip or shorten any inspection, test or check required by a contract or procedure, even under schedule pressure.
- **Do not substitute without approval.** Never change materials, parts, tools, processes or assigned workers without proper review and written approval. Unauthorized substitutions create safety and compliance risk.
- **Document accurately.** Record steps, inspections and test results truthfully. Do not sign for work you did not perform or change records to make them look better.
- **Report nonconforming conditions.** If something does not meet requirements, stop work if needed and report it right away. Do not ship or use nonconforming material unless it goes through the proper review and approval process.
- **Support audits and reviews.** Cooperate with internal audits and customer reviews. Provide honest, complete information and help identify improvements.

Commitment in Action

Q: We are behind schedule, and a coworker suggests skipping a required test and signing off anyway. What should I do?

A: Do not skip tests or sign for work not done. Report the issue to your manager, Quality, Legal or the DRS Alertline.

Related Resources

CON-013 Product Substitution
EHS-001 Environmental Health and Safety

Competing Fairly

We Win Business the Right Way

DRS wins business through our technology, service and people — not through improper agreements or favors. Antitrust and fair-competition laws ban conduct that harms competition, such as price fixing, bid rigging and dividing markets. Even brief conversations with competitors can create serious legal and business risk.



Competitive Intelligence Done Right

Understand our markets and competitors — but gather information the right way.

- Use public sources such as websites, reports, trade journals and open industry events.
- Do not ask customers or suppliers for a competitor's confidential information.
- Never use deception, hacking or pressure to obtain information.

How We Serve

- **Never fix prices or rig bids.** Do not agree with competitors to raise, lower or hold prices, limit output, rotate bids or divide customers or territories.
- **Do not share sensitive information.** Do not discuss prices, discounts, costs, margins, sales or production plans, forecasts or market strategies with competitors. Walk away if talk moves in that direction.
- **Use care in teaming and joint bids.** Teaming can be lawful but may raise risk. Involve Legal early and ensure required disclosures are made to customers.
- **Be careful at industry events.** Keep discussions with competitors general and high level. Stop the conversation and report it to Legal if pricing or other sensitive topics arise.
- **Respect competitor information.** Do not seek or use a competitor's nonpublic information unless Legal approves the way it was obtained and how it will be used.
- **Ask before acting.** If you are unsure whether a discussion or arrangement is allowed, pause and get guidance from Legal.

Commitment in Action

Q: A competitor suggests agreeing on a price floor at a trade show. What should I do?

A: End the conversation, say you cannot discuss pricing and report the incident to Legal or the DRS Alertline.

Related Resources

LEG-003 Antitrust

CON-010 Prevention of Collusive Bidding

Giving and Receiving Gifts Responsibly

We Keep Business Decisions Free from Favor

DRS competes based on our products, services and people — not personal favors. Gifts, meals and other courtesies can support relationships, but they can also create pressure or the appearance of special treatment. Do not give or accept anything that could influence, or appear to influence, a business decision or violate law or policy.

How We Serve

- **Use extra care with government officials.** Never offer or provide anything of value to U.S. or foreign government officials unless approved in advance by Legal or the Ethics and Business Conduct Office.
- **Follow strict limits with suppliers and vendors.** Procurement, purchasing and supply chain employees may not give to or accept gifts or entertainment from suppliers. Others involved in a procurement may not accept gifts or entertainment during that activity.
- **Keep commercial gifts modest.** For private-sector customers and partners, give or accept only modest, occasional business courtesies that:
  - Comply with the law and DRS policy.
  - Are reasonable, business related and properly recorded.
- **Do not solicit gifts or favors.** Never ask suppliers, customers or others for gifts, entertainment, travel or personal discounts.
- **Ask before acting.** If you are unsure whether something is allowed, ask your manager, Legal or the Ethics and Business Conduct Office before you act.

Commitment in Action

Q: A long-time supplier sends me sports tickets worth more than $100 to “thank you for the partnership.” I am not in procurement, but I help advise on supplier choices. What should I do?

A: Do not keep the tickets. Because you influence supplier decisions, accepting a valuable gift could appear to be a conflict of interest and may violate our gifts policy. Thank the supplier, explain that DRS rules do not allow you to accept the tickets, and return them — or otherwise follow guidance from Legal or the Ethics and Business Conduct Office.



Customer Property

Customers may place equipment, tools or other property in our care. Handle this property according to contract terms and use it only for approved business purposes.

- Follow customer instructions for government-owned or customer-furnished property.
- Do not discard or dispose of customer property without written consent and required approvals.
- Protect property from theft, damage, loss or misuse, and do not remove or alter it without authorization.
- Report any loss, damage or misuse right away so DRS can respond.

Related Resources

EBC-003 Restrictions on Gifts, Entertainment or Business Courtesies
EBC-006 Government Relations, Political Activities and Lobbying
CON-005 Prohibition of Bribes and Kickbacks
CON-014 Government Property

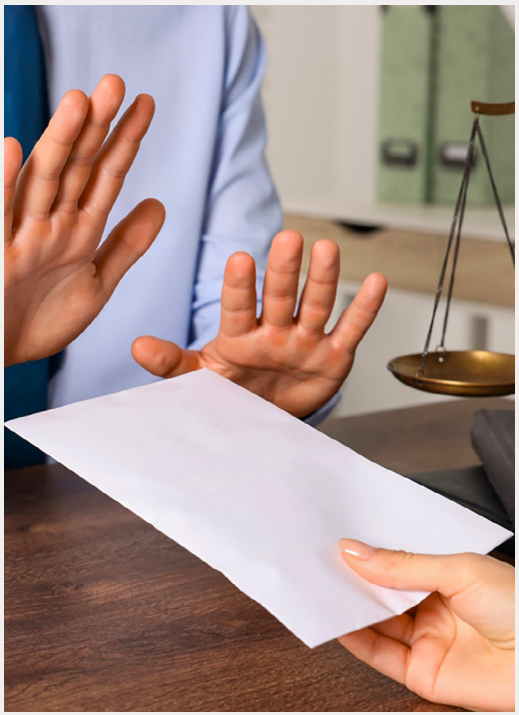
Preventing Bribery and Corruption

We Act with Integrity in Every Business Decision

DRS wins business based on merit — not hidden payments or favors. Bribery, corruption and tax evasion are illegal and violate our values. Anti-corruption laws, including the Foreign Corrupt Practices Act (FCPA) and UK Bribery Act, prohibit us, and any third parties acting for us, from giving or offering anything of value to influence business decisions.

How We Serve

- **Do not offer or accept bribes or kickbacks.** Never give, request or accept anything of value to influence a decision or gain an improper advantage.
- **Do not make facilitation payments.** Small "grease" payments to speed routine government actions are prohibited, even if local law allows them.
- **Use third parties carefully.** Work only with approved agents and consultants. Do not agree to unusual fees or payments without due diligence and Legal approval.
- **Avoid tax evasion.** Do not hide or misstate payments or help others avoid lawful taxes. Ask Legal or Finance if a payment or structure seems unclear.
- **Keep records accurate.** Ensure all payments and discounts are lawful, documented and recorded. Do not create side deals or accept or spend off-the-record funds.
- **Ask before you proceed.** If something feels risky or unclear, pause and get guidance from Legal or the Ethics and Business Conduct Office.



Commitment in Action

Q: A consultant asks for a "special fee" to speed paperwork with a government office. They say it is normal in that country. What should I do?

A: Do not make the payment. Tell them DRS does not allow it and report the request to Legal or the Ethics and Business Conduct Office.

Definitions

- **Bribe:** Anything of value offered or given to improperly influence a decision
- **Kickback:** A payment or benefit given in return for awarding or steering business
- **Foreign government official:** An employee or representative of a foreign government, military, agency or political party, including candidates for office

High-Risk Third Parties

Third parties can create corruption, compliance or tax risks if they are not properly screened and monitored. DRS uses a due diligence process that includes risk-based reviews, clear contract requirements and anti-corruption training for relevant third parties.

- Use only approved intermediaries who pass due diligence.
- Watch for vague services, high commissions or pressure to use unusual payment routes.
- Do not accept payment structures you cannot explain or document.
- If a third party resists compliance checks or asks you to ignore policy, stop and get help.

Related Resources

CON-005 Prohibition of Bribes and Kickbacks
CON-104 Compliance with International Anti-Corruption Laws
CON-022 Compliance with U.S. Sanctions Regulations
CON-020 Restrictive Trade Practices (Antiboycott Regulations)
EBC-003 Restrictions on Gifts, Entertainment or Business Courtesies

Avoiding Insider Trading

We Never Trade on Nonpublic Information

DRS employees may learn important information before it becomes public. U.S. securities laws prohibit buying or selling stock — or sharing information with others — if that information could affect an investor's decision and has not been publicly released.

How We Serve

- **Do not trade on material nonpublic information.** Never buy or sell stock in DRS or any other company if you know information about the company that is material and not public.
- **Do not share nonpublic information.** Do not tell family, friends or others about nonpublic information. Sharing inside information ("tipping") is illegal.
- **Be careful where you talk.** Do not discuss nonpublic information in public places or online where others may overhear or see it.
- **Follow disclosure rules.** If material nonpublic information is shared accidentally, notify Legal immediately so the company can disclose it as required.
- **Ask Legal before you trade.** When unsure whether information is public or material, treat it as nonpublic and confidential, and confirm with Legal before you proceed.



Talking About DRS Outside Work

Simple conversations can create insider trading risk if handled carelessly.

- Keep work discussions factual and high level.
- Never share nonpublic details about earnings, contracts, leadership changes or other sensitive topics.
- If asked about company performance, rely only on public information or decline to answer.

Definitions

- **Material information:** Information a reasonable investor would consider important when deciding to buy or sell stock
- **Nonpublic information:** Information not released to the public or reported through official channels
- **Insider trading:** Buying, selling or recommending a stock while having material nonpublic information, or sharing that information with others ("tipping")
- **Selective disclosure:** Sharing material nonpublic information with certain people — such as analysts or investors — before public release

Commitment in Action

Q: I overheard news about a major contract win that has not been announced yet. Can I buy shares before this news becomes public?

A: No. Buying or selling stock while you have material nonpublic information is insider trading, even if you learned it informally. Do not trade until the information is publicly released and the market has had time to absorb it. If unsure, ask Legal before acting.

Related Resources

LEG-001 Insider Trading
LEG-006 Regulation Fair Disclosure
LEG-007 External Communications

Acting Ethically in Government Contracting

We Serve the Government Ethically

As a U.S. government contractor, DRS must follow strict rules at every stage of our work. Even small lapses can create serious legal, financial or reputational risk and can lead to false claims, loss of contracts or other penalties. Each of us must act with honesty, accuracy and care in everything we do.

How We Serve

- **Follow procurement integrity rules.** Do not seek or use nonpublic government information, including source-selection or competitor proposal data. Never ask for or accept information you are not authorized to receive.
- **Avoid suspended or debarred parties.** Do not work with individuals or companies that are suspended, debarred or otherwise restricted. If something raises concern, stop and check with Legal.
- **Prevent false or misleading claims.** Ensure all records, certifications, proposals, invoices and updates you help prepare are truthful, current and complete. Even small errors or outdated information can result in false claims and serious consequences.
- **Charge labor correctly.** Record your time daily and charge it to the correct project or cost objective. Never move hours to match a budget or hide overruns.
- **Follow rules for hiring former government employees.** Follow required steps before discussing jobs with current or former government employees. Some roles carry strict limits if a government employee is hired.
- **Protect government property and data.** Follow rules for using, marking, storing and returning government-owned or -furnished items and information.
- **Avoid organizational conflicts of interest.** Do not take part in work that could give DRS an unfair advantage or affect our ability to provide objective support. Raise potential issues early.
- **Ask questions early.** If something seems unusual — a payment structure, a proposal change or a request for information — pause and ask Legal before moving forward. Your diligence helps prevent false claims and protects our contracts.

Proxy Compliance

Because DRS is owned by a foreign parent, we follow a Proxy Agreement that allows us to work on classified programs. Use approved channels for required communications with Leonardo representatives, document those communications as instructed and ask Security or Trade Compliance if you are unsure what needs approval.

Definitions

- **Organizational conflict of interest:** A situation where DRS may gain an unfair advantage or may not be able to provide impartial services because of other work or relationships
- **False claim or false statement:** Any request for payment or report to the government that is deliberately untrue, incomplete or misleading, including altered records or hidden facts that affect price or payment

Commitment in Action

Q: A partner offers to share “how our proposal ranked” in a recent competition. What should I do?

A: Do not accept or review it. It may contain nonpublic government or competitor information. Decline the offer and report it to Legal or the Ethics and Business Conduct Office.

Related Resources

CON-003 Truthful Cost or Pricing Data
CON-007 Procurement Integrity
CON-011 Prevention of False Claims and False Statements
CON-015 Organizational Conflicts of Interest
CON-019 Denied and Restricted Parties Screening
EBC-005 Employment Discussions with and Hiring U.S. Government Personnel
FIN-16.4 Labor Charging
SEC-002 Technology Control Plan
SEC-003 Visitor Control Policy
SEC-004 Electronic Communications Plan

Handling Classified Information

We Safeguard What Protects Our Nation

DRS works with classified information and other sensitive government data. These materials must be handled exactly as U.S. government rules require. Protecting this data is essential to national security and to our ability to work on classified programs.

How We Serve

- **Follow all security procedures.** Handle, store, send and destroy classified information only as allowed by the National Industrial Security Program Operating Manual (NISPOM), contract terms and DRS security policies.
- **Respect need-to-know.** Only people with the right clearance and a legitimate need may access the information. Do not share it with anyone unauthorized.
- **Use approved systems and spaces.** Work with classified information only in approved areas and on approved systems. Do not discuss sensitive information in public places, on unsecured calls or in unapproved tools.
- **Control devices in restricted areas.** Do not bring phones, cameras or other unauthorized recording devices into areas where classified information may be present unless approved by Security.
- **Secure information when you step away.** Lock up material in an approved container when not in use. Do not leave it on desks, printers, whiteboards or in meeting rooms.
- **Report problems right away.** If you see or suspect a security issue — such as unattended material, suspicious contacts or unauthorized access — contact your Facility Security Officer (FSO) or Security immediately. Do not try to fix or hide the issue.
- **Cooperate with searches and inspections.** Work areas, storage and personal items at DRS facilities may be searched under company policy and government rules.

Definitions

- **Classified information:** Information marked Classified, Confidential, Secret or Top Secret that the U.S. government protects for national security reasons
- **Need-to-know:** The rule that a cleared person may access information only when required to do their job.



Commitment in Action

Q: I found a folder marked “Classified” left on a conference room chair after a meeting. I am cleared, but I was not part of that meeting. What should I do?

A: Do not open or read the folder. Stay with it and contact your FSO or Security immediately. They will secure the material and determine next steps. Do not leave the folder unattended or remove the folder from the facility.

Related Resources

SEC-002 Technology Control Plan
SEC-003 Visitor Control Policy
SEC-004 Electronic Communications Plan
NISPOM (32 CFR Part 117)

Complying with Trade Laws

We Follow Trade Rules Wherever We Do Business

DRS operates in many countries and must follow U.S. and foreign laws on exports, imports, sanctions and boycotts. These rules apply to hardware, software, technology, services and many routine interactions with foreign persons. Breaking trade laws can lead to fines, loss of export privileges, lost contracts and even criminal charges.

How We Serve

- **Know when an export occurs.** Activities such as sharing controlled technical data with a foreign person, posting sensitive information online or carrying data across borders may all count as exports.
- **Screen business partners.** Work with Trade Compliance to screen customers, suppliers and intermediaries before engagement and as required over time. Do not bypass or ignore a screening hit.
- **Do not proceed with denied or restricted parties.** If screening raises concerns or a party appears on a sanctions, denial or debarment list, stop the engagement and contact Trade Compliance or Legal.
- **Get approvals before exporting.** Do not ship controlled items or share controlled technical data or services without the correct classification, license or authorization.
- **Protect controlled technical data.** Follow the Technology Control Plan. Limit access to authorized people with a need to know and use approved tools when foreign persons visit or join meetings.
- **Watch for boycott language.** Do not agree to contract terms or requests that ask us to avoid certain countries, customers or goods. Send any potential boycott request to Trade Compliance or Legal right away.
- **Document and ask early.** Keep required records. If a transaction, routing or clause seems unusual, pause and ask Trade Compliance or Legal. Report suspected export, sanctions or boycott issues immediately.

Commitment in Action

Q: A customer wants a fast quote and asks us to confirm that none of our products involve a certain country. Screening is not done. Can I sign?

A: No. It may be a boycott request. Explain that screening must come first and do not sign or ship. Send the request to Trade Compliance and Legal.



Definitions

- **Export:** Sending to or sharing controlled items, software or technical data — inside or outside the U.S. — with a foreign person
- **Foreign person:** Anyone who is not a U.S. person, including most foreign companies or governments
- **Denied/restricted party:** A person or entity restricted or prohibited by sanctions or debarment lists
- **Boycott request:** A request to avoid certain countries or to certify that we do not do business with them

Related Resources

TCO-100 Trade Compliance
TCO-122 Politically Sensitive Transactions
CON-019 Denied / Restricted Parties Compliance Screening
CON-020 Restrictive Trade Practices (Antiboycott Regulations)
SEC-002 Technology Control Plan

Preventing Money Laundering

We Watch for Suspicious Transactions

Money laundering takes money from crime and makes it appear legitimate. It can support fraud, drug trafficking and terrorism. DRS must follow U.S. anti-money laundering laws, and we must not be used — directly or indirectly — to move or hide criminal funds.



How We Serve

- **Know your customers and deals.** Be alert to the true identity of the party we are doing business with, how they pay and how they use our products and services.
- **Watch for unusual payments.** Question complex structures, cash payments, transactions involving high-risk locations or requests to route money through unnecessary intermediaries.
- **Check documents for accuracy.** Look for unusual pricing, inconsistent quantities or vague descriptions in contracts, invoices, shipping or tax documents.
- **Report concerns right away.** If a transaction or payment "does not look right," report it to your manager, Legal, Designated Corporate Counsel or the DRS Alertline. Do not ignore or try to fix it yourself.

Commitment in Action

Q: A new customer insists on paying for a large order through several small transfers from different accounts, even though a normal bank transfer would be easier. It feels odd. What should I do?

A: Do not treat this as routine. Tell your manager and notify Legal, Designated Corporate Counsel or the DRS Alertline. Explain what you observed and share any documents. They will determine whether the activity must be reported and whether the transaction can proceed.

Related Resources

CON-021 Compliance with U.S. Regulations on Money Laundering

Managing Third-Party Risks

We Expect Partners to Meet Our Standards

DRS works with many third parties — consultants, sales representatives, service providers and others — who must follow the same laws and ethical standards we do. We do not use third parties to avoid rules or gain improper advantage.

How We Serve

- **Choose partners carefully.** Work with Legal or Trade Compliance to review a third party's reputation and compliance history. Do not begin work with the third party until checks are complete.
- **Screen for restricted or high-risk parties.** Screen customers, suppliers and intermediaries before engagement and as required. Do not work with anyone who does not pass screening.
- **Use clear written agreements.** Use contracts approved by Legal or Contracts and ensure they allow DRS to end the relationship if laws or policies are violated.
- **Do not bypass rules through others.** Never ask or allow a third party to do something DRS is not permitted to do, such as offering improper gifts or seeking protected information.
- **Watch for warning signs.** Be alert to vague services, unusual payment routes, reluctance to complete due diligence or signs of unethical conduct.
- **Report concerns quickly.** If a third party refuses screening, requests improper payments or seems to break rules, stop work and contact Legal, Trade Compliance or the Ethics and Business Conduct Office.

Definitions

- **Third party/intermediary:** Any non-DRS person or organization acting for DRS, such as representatives, agents or service providers
- **Due diligence:** Checks to confirm a third party is qualified, trustworthy and able to follow laws and DRS policies



Commitment in Action

Q: A sales representative wants payment through a new "associate company" and has not completed screening. What should I do?

A: Do not proceed. Tell them screening is required and notify Legal or Trade Compliance.

Related Resources

CON-102 International Service Providers
CON-104 Compliance with International Anti-Corruption Laws
CON-019 Denied / Restricted Parties Compliance Screening
CON-005 Prohibition of Bribes and Kickbacks
EBC-003 Restrictions on Gifts, Entertainment or Business Courtesies
CITG-002: Program Data Governance Policy

Respecting Human Rights

We Honor and Defend Human Rights

DRS is committed to respecting human rights across our operations and working with partners who do the same. We strictly prohibit forced labor, slavery, human trafficking and any form of exploitation. As a defense technology leader, we support security and freedom by ensuring our products, services and partnerships never contribute to abuse.

How We Serve

- **Reject all forms of exploitation.** Never use or tolerate forced, bonded or child labor in any form, whether within DRS or through business partners.
- **Ensure fairness in recruitment and employment.** Use truthful hiring practices, do not charge recruitment fees or withhold identity documents and make sure wages, benefits and working conditions meet or exceed legal requirements.
- **Choose partners who share our standards.** Establish the expectation with suppliers and contractors to comply with our Supplier Code of Conduct. Set clear expectations and support compliance through due diligence and supplier reviews.
- **Respect workers' rights.** Support freedom of association, lawful working hours and safe, healthy working conditions.
- **Stay alert and speak up.** Report any suspected human rights violations — inside DRS or in our supply chain — to management, Legal or the DRS Alertline. Retaliation for good-faith reports is prohibited.
- **Lead with dignity and respect.** Treat everyone with respect, honoring our commitment to empowerment, inclusion and the wellbeing of others.



Definitions

- **Forced labor:** Making someone work against their will or through threats, coercion or abuse of authority
- **Human trafficking:** Recruiting, transporting or harboring people through force, fraud or coercion for exploitation
- **Child labor:** Employing anyone below the minimum legal working age or in work that harms the child's health, safety or education, even if above that minimum

Commitment in Action

Q: During a supplier visit, I learned that some workers paid high recruitment fees to secure their jobs. The supplier says this is "normal practice" in their country. What should I do?

A: Raise the concern right away. Recruitment fees can lead to debt bondage — a form of forced labor. Notify your business unit leader or the DRS Alertline. Our policies and Supplier Code of Conduct require suppliers to use fair hiring practices and prohibit any form of forced or exploitative labor.

International Standards

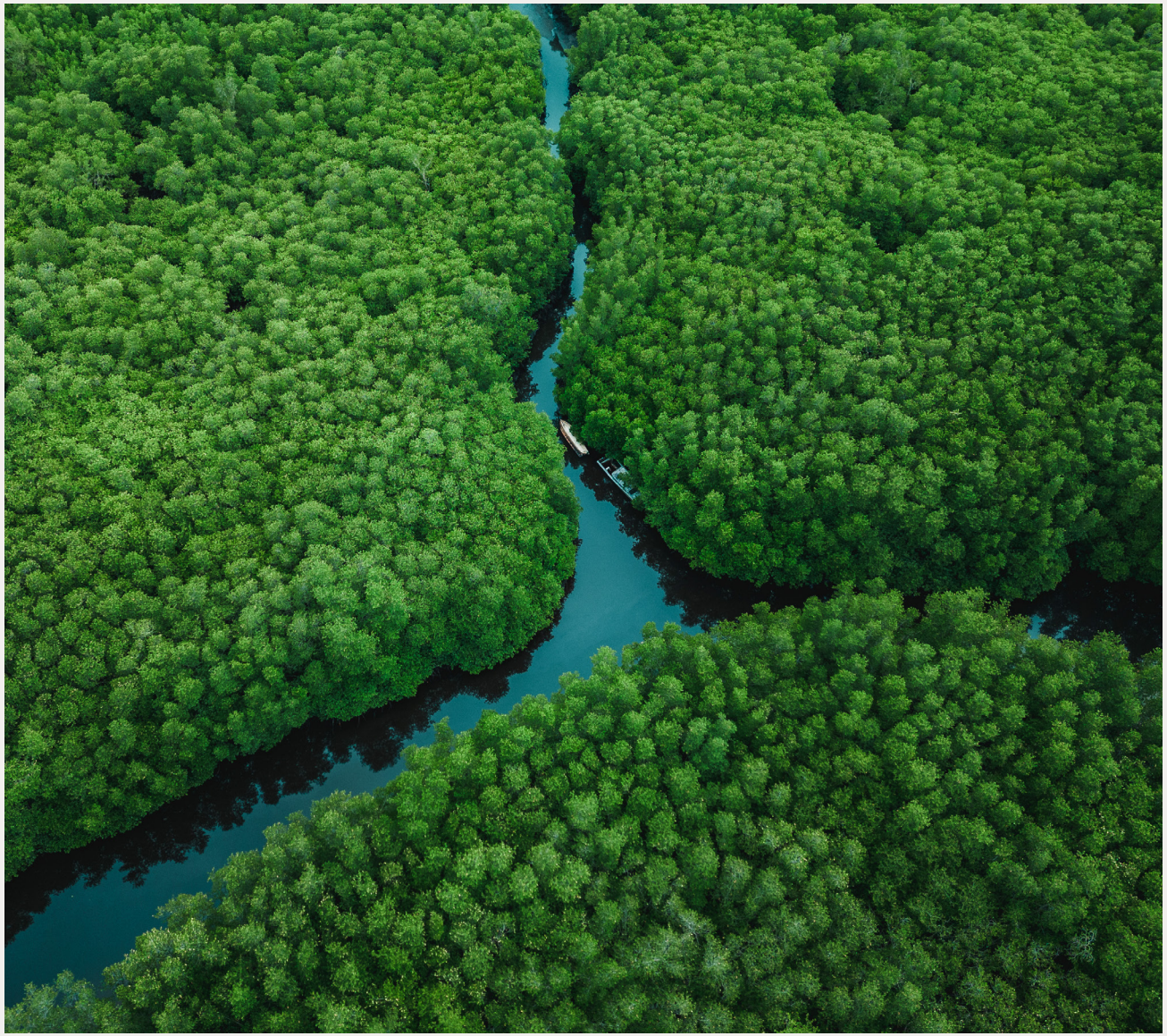
Our approach is informed by leading global frameworks, including the UN Guiding Principles on Business and Human Rights, the OECD Guidelines for Multinational Enterprises and the International Labour Organization's core labor principles.

Related Resources

CON-002 Combating Trafficking in Persons Policy
Statement on Preventing Forced Labor in Our Operations (2025)
Supplier Code of Conduct

Protecting the Environment

We Respect People, Planet and Performance



DRS is committed to protecting the environment. We follow environmental laws, prevent pollution, conserve resources and operate safely.

How We Serve

- **Follow environmental rules.** Know the requirements for your site and job.
- **Use resources wisely.** Reduce waste and emissions and support recycling.
- K**eep areas safe and clean.** Store chemicals and waste properly. Do not ignore leaks, spills or unsafe conditions.
- **Report issues immediately.** If you see a spill, release or unsafe condition, tell your manager, EH&S coordinator or Site Management.

Commitment in Action

Q: I notice a small leak from a waste container near the loading dock. Someone put a rag under it. Do I need to report it?

A: Yes. Any leak or spill that could reach soil, drains or groundwater must be reported and cleaned up properly. Tell your manager or EH&S coordinator right away.

Related Resources

EHS-001 Environmental Health and Safety

Supporting Our Communities

We Contribute Where We Live and Work

DRS works to be a positive presence in the communities where we operate. We show this through our conduct, volunteer efforts and support for local partners. Our actions should reflect respect, fairness and care for the people and places around us.



How We Serve

- **Act as a responsible neighbor.** Treat people with courtesy and support safe operations that protect local health, safety and the environment.
- **Volunteer thoughtfully.** Join company-supported programs when you can, ensuring participation does not interfere with your job or create a conflict of interest.
- **Use company resources properly.** Do not use company funds, equipment or time for community or charitable activities unless approved under company guidelines.
- **Raise concerns.** If a community activity or partnership seems inconsistent with our values or could create risk, speak up to your manager, Legal or the Ethics and Business Conduct Office.

Commitment in Action

Q: A community group wants me to speak as a DRS employee and comment on business plans. What should I do?

A: Get approval before speaking. Do not represent DRS or discuss business plans without written authorization from Legal.

Related Resources
LEG-007 External Communications

Engaging in Political Activity Responsibly

We Keep Personal Politics Separate from DRS



We respect your right to engage in politics. At the same time, DRS must follow lobbying and campaign finance laws and keep company resources out of partisan activity unless clearly approved.

How We Serve

- **Keep personal and company roles distinct.** Do not use DRS money, systems, logos, facilities or work time for political campaigns, candidates or parties unless you have written approval.
- **Recognize that PAC giving is voluntary.** The DRS PAC is funded only by employees who choose to contribute. Never pressure anyone or suggest political support affects employment or opportunities.
- **Coordinate communications with officials.** Before contacting members of Congress, their staff or senior executive branch officials about laws, policies or official DRS business, get approval from Government Relations.
- **Know what counts as lobbying.** Meetings, calls, emails and prep time with covered officials about laws, regulations, programs or contract decisions may be lobbying. Lobbying activity must be approved by Government Relations, and related time and expenses must be recorded accurately.
- **Use only approved lobbyists and advisors.** Do not hire or direct outside lobbyists, consultants or law firms to reach out to government officials for DRS without required approvals.

Commitment in Action

Q: I am working on a proposal and want to call a Congressional staff member I know to explain why our solution is better. Can I reach out?

A: Not on your own. Contacting legislative government officials about DRS business or policy issues may be considered lobbying and must be coordinated and approved in advance. Contact Government Relations or Legal before taking any action so they can guide you and ensure proper reporting.

Related Resources

EBC-006 Government Relations, Political Activities and Lobbying
GREL-001 Coordination with Government Relations
EBC-003 Restrictions on Gifts, Entertainment or Business Courtesies

Responding to Media and Government Inquiries

We Share Accurate Information Through the Right Channels

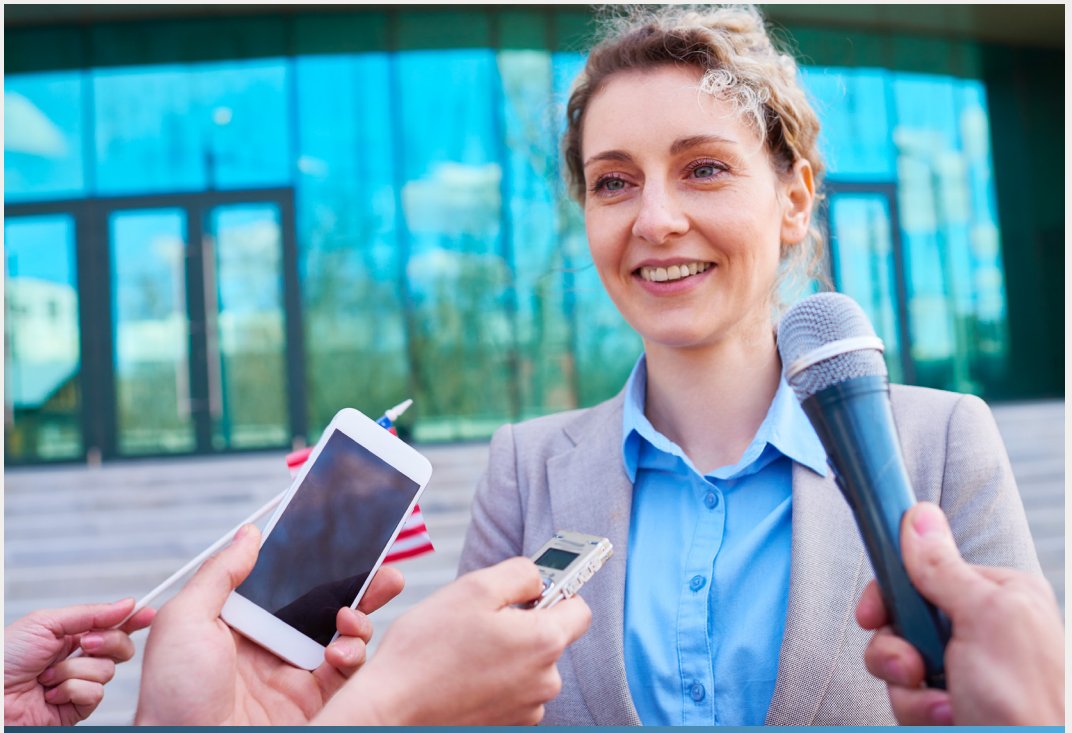
What we say in public can affect DRS's reputation, contracts and legal duties. Only authorized people may speak for DRS, and all of us must route outside questions through the right channels.

How We Serve

- **Let authorized spokespeople speak for DRS.** Do not give statements about DRS business to reporters, investors, analysts, regulators or industry groups. Send all requests to Communications or Legal.
- **Route government questions correctly.** If you receive a call or email from a government customer, regulator or other authority that goes beyond normal contract work, follow your site process and contact Legal, Government Relations or your business leader.
- **Coordinate with Government Relations.** Before talking with covered federal officials or state elected officials about laws, policies or DRS issues, obtain approval from and work through Government Relations so they can guide and track the contact.
- **Keep internal messages inside DRS.** Treat internal emails, slides and talking points as CCI or confidential information. Do not forward or post them externally unless Communications or Legal has cleared them.
- **Ask before you speak in public.** Get approval from Public Relations and Legal before giving interviews, writing articles or joining events where people may see you as a DRS representative.
- **Report mistakes quickly.** If you see nonpublic, incorrect or misleading information about DRS outside the company, contact Legal or Communications right away. Do not attempt to correct it yourself.

Definition

- **Authorized spokesperson:** Someone DRS has formally approved to speak on behalf of the company



Commitment in Action

Q: A reporter calls and asks for a comment about a recent DRS contract award. Can I confirm it?

A: No. Take the reporter's name and contact details and refer them to Communications or Legal. Only authorized spokespeople may talk to the media for DRS.

Related Resources

LEG-007 External Communications
SEC-004 Electronic Communications Plan
GREL-001 Coordination with Government Relations

Using Social Media with Care

We Use Our Voice Responsibly



Commitment in Action

Q: I want to post a photo from work on my personal social media. Is that okay?

A: Maybe not. Photos can reveal sensitive details. Check with your manager or Security before posting.

Social media refers to any online platform where people share, view or respond to content, such as LinkedIn, X, Facebook, Instagram, YouTube, blogs and forums. Such forums connect us, but posts made about our work or industry can affect DRS's reputation and create security, privacy or legal risks. We support personal expression, but we must use care when sharing anything that could be tied to DRS.

How We Serve

- **Think before you post.** Pause before posting, liking or sharing content related to DRS or our customers or industry.
- **Protect confidential information.** Never share CCI without prior authorization.
- **Keep logos and branding secure.** Do not use company logos or create accounts or pages that appear to represent DRS without approval.
- **Speak only for yourself.** Make clear your views are your own. Do not imply DRS supports any political candidate, cause or opinion.
- **Stay respectful online.** Avoid posts that could be seen as harassing, discriminatory or harmful.
- **Ask if you're unsure.** If speaking or appearing online could link you to DRS, check first with your manager, Communications or Legal.

Related Resources

HR1011 Social Media Policy
CITG-001 Cyber / IT Acceptable Use Policy

Code of Ethics and Business Conduct

© 2026 Leonardo DRS, Inc. All rights reserved.

LEONARDO DRS



Leonardo DRS Ethics and Business Conduct Office
Leonardo DRS Alertline:
Toll free at 1-800-694-5005
Online at https://drs.alertline.com

Regular mail:
Leonardo DRS Ethics and Business Conduct
2345 Crystal Drive, Suite 1000
Arlington, VA 22202