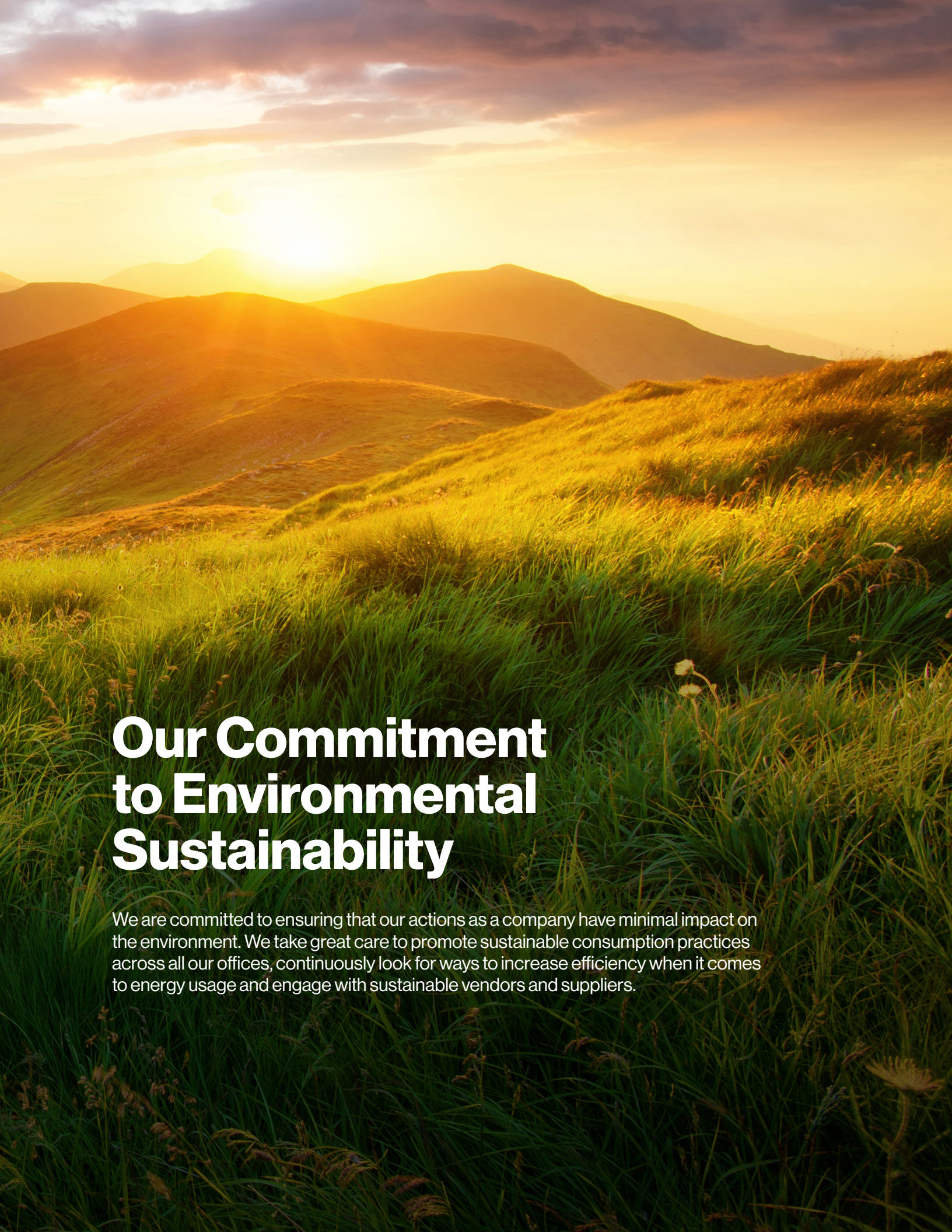
Ruder Finn Group Policies

ruderfinn



Our Commitment to Environmental Sustainability

We are committed to ensuring that our actions as a company have minimal impact on the environment. We take great care to promote sustainable consumption practices across all our offices, continuously look for ways to increase efficiency when it comes to energy usage and engage with sustainable vendors and suppliers.

Our Sustainable Consumption and Practices

We have a ban on single use plastic.

We have removed all single-use plastic from our offices, replacing it with glass and non-single use plastic items in common areas and promoting the use of glass water and drink pitchers over individual plastic bottles. We are also conscious of the amount of plastic used when it comes to take-out and catering, opting out of plastic utensils and other single-use items, and we encourage our employees to do the same.

We minimize waste and recycle what we can.

In 2019, we replaced all of our individual garbage bins with a more centralized bin on each floor and provided recycling bins for paper, cardboard and plastic. All of the paper and cardboard we purchase is recycled paper and all toners and ink cartridges are recycled through original equipment suppliers.

We reuse as long as possible.

We follow a "re-use" model for all IT equipment and once the piece of equipment is at its end of life, we donate it to NGOs and local schools.

We prioritize efficient energy use.

We employ a business management system that regulates light, A/C and heat usage and we only purchase and use energy star appliances and fuel-efficient equipment. Our clock, day light and occupancy sensors provide automatic on and off functionality to preserve energy.

We promote sustainable travel.

We ask that employees push for virtual meetings over business travel and leave business travel only for essential needs. We also encourage employees to take advantage of public transportation and car-pooling.

Employee Engagement & Volunteerism

At Ruder Finn, we partner with many non-profits in the cities where our employees live and work. Whether it's collecting and donating food and clothing for homeless shelters, or holiday gift giving for children in need, we believe in giving back to the community. We also encourage and provide time off for all employees to pursue volunteer activities outside of work to advance issues important to them.

Furthermore, the Ruder Finn Green Team, our dedicated team consisting of employees passionate about the environment provides ongoing education to other employees on new, sustainable measures and how we can adopt them, individually and as a company.

Commitment to the UN Sustainable Development Goals (SDGs):

As global citizens and corporate stewards, Ruder Finn is committed to doing our part to advance the Sustainable Development Goals (SDGs) set by the United Nations. While all the goals are important, we prioritize the SDGs where we can make the biggest impact:

SDG 3: Good Health and Wellbeing

We are actively working with clients across all levels of health and wellness ranging from rare disease, advocating for more equitable access to medicine, and promoting mental health.

SDG 5: Gender Equality

As a woman-led company, Ruder Finn is fully committed to ensuring full and effective participation and equal opportunity for women at all levels of decision making in political, economic and public life.

SDG 10: Reduced Inequality

We are strong advocates of adopting policies that promote greater equality within Ruder Finn, but through our actions, we seek to empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status.

Code of Conduct

Our employees are the most valued part of our company and that is why the health and safety of our employees is our top priority. With that, Ruder Finn is committed to protecting the safety, health and well-being of its employees and all people who use our services and/or who may come in contact with our workplace and property.

Ruder Finn strives to ensure that all individuals associated with the company are treated in a respectful and fair manner. Though it is not possible to list all forms of behavior that are unacceptable in the workplace, the following are examples of behavior that would be considered infractions of Ruder Finn's codes of conduct that is set forth throughout Ruder Finn's 2021 Employee Handbook (please see attached for Ruder Finn's 2021 Employee Handbook. Such behavior may result in disciplinary action, up to and including termination of employment. To that end, the following is a non-exhaustive list of examples of activities that are in direct breach of our 2021 Employee Handbook:

1. Theft or inappropriate removal or possession of company property or the property of a fellow employee.
2. Willful destruction of company property or the property of a fellow employee.
3. Working under the influence of alcohol or illegal drugs.
4. Possession, distribution, sale, transfer or use of alcohol or illegal drugs in the workplace, while on duty or while operating employer-owned vehicles or equipment.
5. Fighting or threatening violence in the workplace.
6. Sexual or other harassment.
7. Using excessively abusive, threatening or obscene language.
8. Using intimidation tactics and making threats.
9. Sabotaging another's work.
10. Making malicious, false and harmful statements about others.
11. Publicly disclosing another's private information.
12. Possession of dangerous or unauthorized materials, such as explosives or firearms, in the workplace.
13. Unauthorized disclosure of business secrets, trade secrets, or confidential information.
14. Falsifying company records or reports, including one's time records or the time records of another employee.

Commitment to DE&I

Ruder Finn is an Equal Opportunity Employer that is committed to DE&I. We are committed to a workplace environment that encourages growth and respect for all current and prospective employees based upon job-related factors such as their educational background, work experience, and ability to perform the essential functions of a particular job. It is the policy and practice of Ruder Finn to prohibit any form of discrimination or harassment based on actual or perceived race (including traits historically associated with race, including but not limited to, hair texture and hairstyles such as braids, locks and twists), color, age, citizenship, alienage or national origin, religion, marital status, sexual orientation, sex or gender (including pregnancy, childbirth, breastfeeding or related medical conditions), gender identity or gender expression, military or veteran status, physical or mental disability, genetic information, medical condition (including cancer), or any other status protected under applicable federal, state or local law. Support and belief in this principle is a basic responsibility of all Ruder Finn employees.

Ruder Finn will provide reasonable accommodations as necessary and where required by law so long as the accommodation does not pose an undue hardship. This policy is not intended to afford employees with any greater protections than those which exist under federal, state or local law.

Ruder Finn strongly urges the reporting of all instances of discrimination and harassment, and prohibits retaliation against any individual who reports discrimination, harassment, or participates in an investigation of such report. To this end, Ruder Finn maintains an Ethics Hotline to report any suspected incidences of discrimination, harassment, or other misconduct. Individuals can make a report by contacting Ruder Finn's NAVEX Ethics Hotline at 844-973-0167 or www.ruderfinn.ethicspoint.com. This hotline is available 24/7, 365 days a year, for individuals to confidentially report any issue or suspected incidence of discrimination, harassment, or other misconduct.

Appropriate disciplinary action, up to and including immediate termination, will be taken against any employee who violates our DE&I policies. We believe that our continued success depends upon our ability to maintain a leadership role in the attraction, development and retention of a highly competent work force and to create a climate for effective and productive use of our employees. Our management is guided by ethical standards that comply with legal requirements. These standards will be implemented consistently by Ruder Finn to ensure that equality is afforded to all applicants and employees.

As part of our commitment to a welcoming and inclusive workplace, each employee is required to complete interactive training on both harassment prevention and diversity and inclusion once each calendar year.

Ethics Statement & Anti-Corruption

Ruder Finn strives to maintain our agency's reputation in our industry as leader in the commitment to an excellence in ethics and business conduct. The purpose of our Ethics Committee is to clarify the elements of an ethical issue and make recommendations to the Ruder Finn's Executive Committee when decisions are called for.

This Code of Ethics is used for deliberations by the Ethics Committee. It makes explicit those beliefs and tenets which have long been assumed as inherent in the character and culture of Ruder Finn, including without limitation compliance with any and all applicable anti-corruption laws, including without limitation "any foreign or domestic anti-bribery and anti-corruption laws, statutes, ordinances, codes, rules, regulations, standards, orders, and other governmental requirements having the force of law both in the U.S. and outside the U.S., including but not limited to the UK Bribery Act 2010, the US Foreign Corrupt Practices Act 1977, as amended, and any laws intended to implement the Organization for Economic Co-operation and Development ("OECD") Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions, applicable to the Company or its operations anywhere in the world. In order to maintain these high ethical standards, Ruder Finn works to ensure that all employees are informed about anti-bribery and anti-corruption guidelines and best practices. As such, we have a mandatory Anti-Bribery & Anti-Corruption training that employees must complete yearly.

Furthermore, Ruder Finn takes the following position pertaining to ethics and compliance with Anti-Bribery and Anti-Corruption laws:

1. We take ethics seriously.
2. We always strive to achieve the highest level of professional excellence in the work we do for clients. We want to be – and be known as – an agency that provides intelligent, thoughtful and creative service in an ethical manner.
3. We want to be proud of the clients we represent.
4. We want to feel that we are performing a useful function for society as well as for our clients.
5. We want to avoid conflicts of interest. When we identify a potential conflict of interest between clients, our policy is to disclose the matter to both clients. In making our decision as to whether or not to resign an account, we take into consideration ethical standards in our industry, our clients' concerns, our responsibility to both clients, the history of our relationship, as well as the scope of the program.
6. We want to respect the individual concerns of those who work for the firm and those for whom we work and encourage a sense of loyalty and responsibility to each other.

7. We realize that an organization as large as ours includes individuals with as many different opinions as there are issues. It is our policy that no individual should be required to work on an account with which he or she feels uncomfortable. At the same time, we feel that it is up to management to determine the kind of clients the company should represent. Management may be advised through discussions with the Ethics Committee as to the considerations involved in any controversial issue.

8. We recognize that in a democracy, everyone has the option to be represented by an advocate. Our work involves advocacy directed to the public (or a specific segment of the public), and hence has a bearing on our own beliefs as members of that public. We therefore do not want to represent a client whose policies or actions are contrary to our beliefs or are deemed unethical.

9. We don't want to be involved in any public relations activity that we believe:

   - Violates the confidentiality of a client
   - Defends or endorses the suppression of human rights anywhere in the world, or promotes, however subtly, racism, discrimination, terrorism or other policies which we feel are contrary to our basic beliefs
   - Defends or endorses the suppression of religious freedom
   - Censors the arts
   - Curbs free speech
   - Interferes with crime prevention
   - Threatens world peace
   - Is hazardous to anyone's health
   - Is a threat to the environment
   - Is scientifically unsafe
   - Is not consistent with our cultural standards of quality
   - Disseminates what we believe is false and deceptive information
   - Makes unsupported or misleading claims for our and our clients' products, corporations, institutions, governments, or causes

10. We want to make sure that employees are aware of the legal/statutory implication of their status as corporate insiders and encourage them to avoid any securities trading (or other inappropriate personal activity) which might be construed as misuse of confidential client information.

11. We want to make sure that in matters related to finance and particularly in regard to billing and expenses, our employees not only abide by Ruder Finn's policies but comply with our client's own company policies.

Every employee is required to acknowledge the Employee Handbook to confirm their understanding of and commitment to comply with the Code of Ethics. If an employee wishes to report a violation of the Ethics Code, the employee can contact Ruder Finn's NAVEX Ethics Hotline at 844-973-0167 or submit a report of a suspected or actual violation at www.ruderfinn.ethicspoint.com. The hotline is available 24/7, 365 days a year, for individuals to confidentially report any issue or suspected incidence of misconduct.

Our Vendor and Supplier Policy

We track all of our vendors and suppliers and have a preferred list of sustainable vendors and suppliers that we prioritize based on their environmental sustainability and diversity, equity and inclusion practices. We regularly ask that all vendors and suppliers fill out a questionnaire on their environmental and societal practices if the information is not readily available.

In all offices, we ensure that the sustainability principles are adhered to. When considering office space, we look for LEED certified buildings.

Employee and Supplier Code of Conduct

Ruder Finn and its subsidiaries operate in many countries throughout the world. This global footprint must always respect local and international laws in all areas where business is conducted. We uphold ourselves to the highest level of ethics, integrity, transparency and honesty regardless of location and we expect our suppliers to have the same commitment.

Our employees and suppliers shall comply with all applicable laws and regulations in the countries and jurisdictions in which they operate. Employees and suppliers may be asked for information requests and/or audits to ensure their fulfillment of responsibilities.

We provide the following minimum standards to our Suppliers (which our employees must follow as well, as applicable):

Labor and Human Rights

Working Hours, Wages, and Benefits

Ruder Finn and its suppliers shall pay workers according to applicable wage laws, including minimum wages, overtime hours and mandated benefits. Ruder Finn and its suppliers shall communicate with the worker the basis on which they are being compensated in a timely manner and are also expected to communicate with the worker whether overtime is required and the wages to be paid for such overtime.

Anti-Discrimination & Anti-Harassment and Abuse

Ruder Finn and its suppliers shall not discriminate against any worker based on age, disability, gender identity or expression, marriage and civil partnership, pregnancy and maternity, race, color, nationality, ethnic or national origin, religion or belief, sex, sexual orientation or any other legally protected characteristic, in hiring or other employment practices. Ruder Finn and its suppliers will not tolerate harassment and abuse and shall not threaten workers with, or subject them to, harsh or inhumane treatment including sexual harassment, sexual abuse, corporal punishment, physical coercion or verbal abuse. Both Ruder Finn and its suppliers shall uphold the human rights of workers and treat workers with dignity and respect and shall ensure that workers have a mechanism to report grievances and that the business encourages and facilitates open communication between management and workers.

Underage Workers

Ruder Finn and its suppliers shall not use child labor. The employment of workers below the age of 18 shall only occur in non-hazardous work and when young workers are above a country's legal age for employment or the age established for completing compulsory education.

Freedom of Association

Ruder Finn and its suppliers shall freely allow workers lawful rights to associate with others, form and join organizations of their choice, and bargain collectively, without interference, discrimination, retaliation or harassment. Open communication and direct engagement with workers to resolve workplace and compensation issues is encouraged.

Employment Status

Ruder Finn and its suppliers shall provide a written contract of employment to their employees and who lawfully live and work in the country in which you operate. Both Ruder Finn and its suppliers shall ensure that all workers provide satisfactory proof of identity to you and that employment by the supplier does not breach any laws, rules or regulations. Suppliers employees should be able to freely leave their employment after giving reasonable notice and are not required to lodge deposits or payments (in cash or other kind) with the supplier. There should be no forced, bonded or involuntary labor.

Prevent of Modern Slavery and Human Trafficking

Ruder Finn and its suppliers shall take reasonable steps to ensure that modern slavery and human trafficking is not taking place in in any part of the business or supply chain. Suppliers may be required to provide a modern slavery and human trafficking report setting out the steps that have been taken to ensure that modern slavery and human trafficking is not taking place in any part of the business. This may include, to the extent relevant, information concerning force, bonded, indentured labor or involuntary prison labor.

Subcontracting

Ruder Finn and its suppliers shall not use subcontractors for the provision of goods or services to us without our prior written consent, and in the event such prior written consent is given by us, suppliers shall require the subcontractor to enter into a written commitment with you to comply with this Employee and Supplier Code of Conduct.

Public Decency

Ruder Finn and its suppliers will not knowingly create work that contains statements, suggestions or images offensive to general public decency and will give appropriate consideration to the impact of our work on minority segments of the population, whether that minority be by race, religion, national origin, color, sex, sexual orientation, gender identity or expression, age or disability.

Whistleblowing

Ruder Finn and its suppliers shall have clear policies and procedures in place so that workers may report concerns about wrongdoing in their workplace without being victimized or dismissed. Both Ruder Finn and its suppliers shall also comply with all other applicable laws in relation to whistleblowing.

Health and Safety

Health and Safety

Ruder Finn and its suppliers shall provide and maintain a safe work environment and integrate sound health and safety management practices into the business. Both Ruder Finn and its suppliers shall have a system for workers to report health and safety incidents without fear of reprisal, as well as a system to investigate, track, and manage such reports, and implement required corrective action. Ruder Finn and its suppliers shall obtain, keep current, and comply with all required health and safety permits, licenses and consents.

Drugs and Alcohol

Ruder Finn and its suppliers will not tolerate the use, possession, or distribution of illegal drugs, or allow employees to report to work under the influence of drugs or alcohol.

Environmental

Environmental

Ruder Finn and its suppliers shall develop, implement and maintain environmentally responsible business practices. Ruder Finn and its suppliers shall implement a systematic approach to identify, manage, reduce, and responsibly dispose of or recycle all your waste. Ruder Finn and its suppliers shall obtain, keep current and comply with all required environmental permits, licenses and consents and comply with any reporting requirements. Ruder Finn and its suppliers shall carry out operations with care for the environment and comply with all applicable environmental laws and regulations.

Ethics and Compliance

Ethics

Ruder Finn and its suppliers shall always be ethical in every aspect of business, including relationships, practices, sourcing and operations and should strive to maintain a high standard of ethics.

Anti-Bribery

Suppliers shall not engage in corruption, extortion, embezzlement or bribery to obtain an unfair or improper advantage. Ruder Finn and its suppliers shall not provide or receive anything of value to obtain an improper business advantage or favorable treatment or exert undue influence, including offering, giving, asking for or taking any form of potential bribe or kick-back. This prohibition extends to payments and gifts of cash or in kind, made directly or through others. Ruder Finn and its suppliers must not offer any potentially illegal payments to, or receive any potentially illegal payments from, any customer, supplier, their agents, representatives or others. This includes a prohibition on facilitation payments intended to expedite or secure performance of a routine governmental action such as obtaining a visa or customs clearance, even in locations where such activity may not violate local law. Ruder Finn and its suppliers shall abide by all applicable anti-corruption laws and regulations of the countries in which they operate.

Disclosure of Information

Ruder Finn and its suppliers shall accurately record information regarding your business activities, employment, health and safety, and environmental practices and shall disclose such information, without falsification or misrepresentation, to all appropriate parties and as required by law. Ruder Finn and its suppliers shall maintain accurate financial books and business records in accordance with all applicable legal and regulatory requirements and accepted accounting practices.

Competition and Anti-Trust

Ruder Finn and its suppliers must comply with all applicable competition laws (sometimes called “antitrust laws”). These laws prohibit formal or informal understandings, agreements or arrangements among competitors that unfairly restrict competition. Ruder Finn and its suppliers must not fix prices, rig bids with your competitors or participate in a cartel. This includes a prohibition on exchanging current, recent or future pricing information with competitors.

Management System

Informational Security

Ruder Finn and its suppliers must comply with applicable data privacy laws and must protect the confidential and proprietary information of others, including personal data, from unauthorized or unlawful processing, access, destruction, use, modification and disclosure, and against accidental loss or destruction, or damage through appropriate technical and organizational measures including physical and electronic security procedures. Ruder Finn and its suppliers are expected to take the necessary information security measures, for both computer systems and portable electronic devices, to protect against malware and unauthorized disclosure of any proprietary information.

Intellectual Property Rights

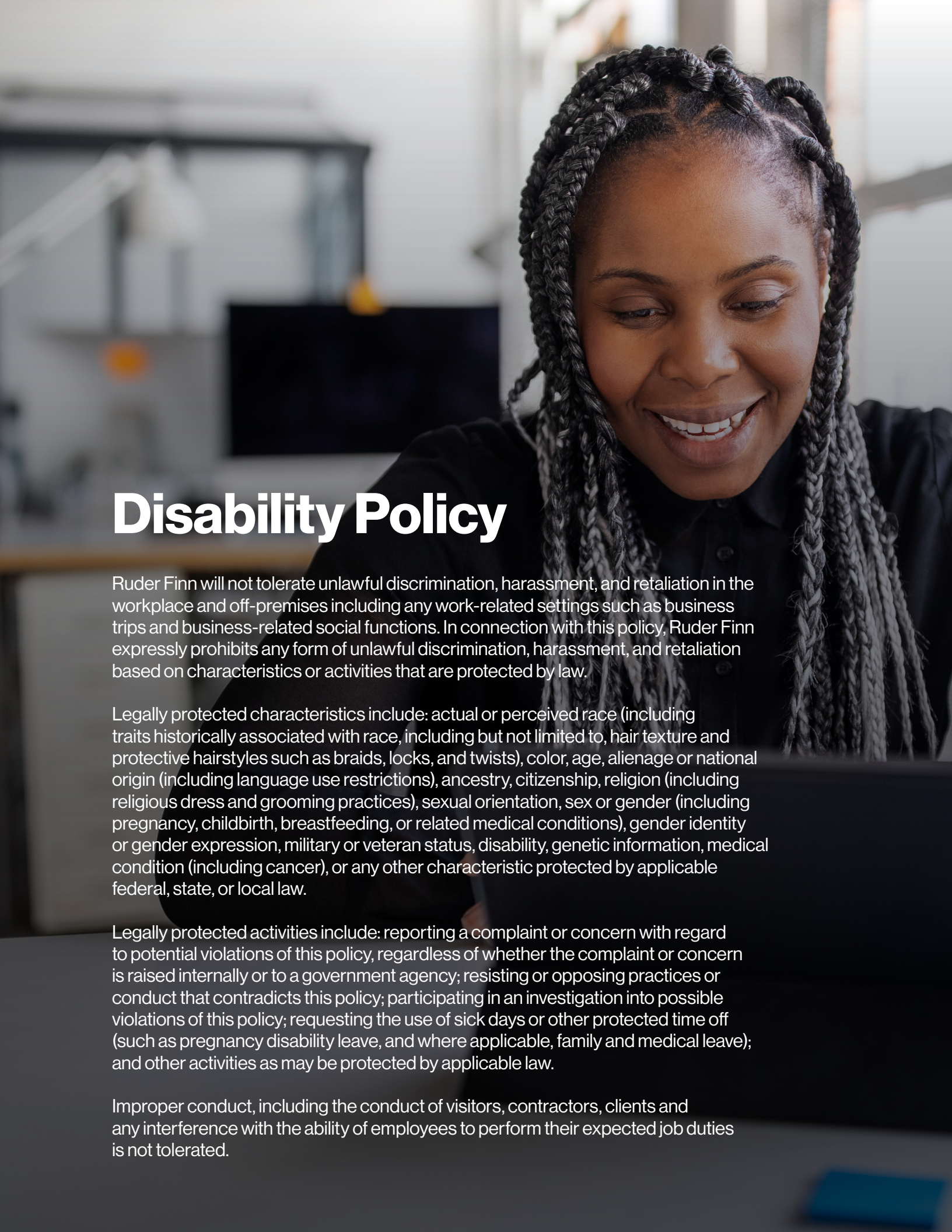
Ruder Finn and its suppliers shall respect intellectual property rights and shall not knowingly infringe the intellectual property rights of any third party. Ruder Finn and its suppliers shall manage technology and know-how in a manner that protects intellectual property rights.

Confidentiality

Ruder Finn and its suppliers shall safeguard our information by keeping it confidential, secure, limiting access, and avoiding discussing or revealing such information in public places. These requirements extend even after the conclusion of your business relationship with us.

Risk Assessment and Management

Ruder Finn and its suppliers shall develop and maintain a process to identify employment and human rights, health and safety, environmental, business ethics, and legal compliance risks associated with your operations, determine the relative significance of each risk, and implement appropriate procedures and controls to minimize the identified risks. They shall have written standards, performance objectives, targets, and implementation plans, including periodic assessments of performance against those objectives. They shall perform periodic evaluations of your facilities and operations, and the facilities and operations of your subcontractors that provide goods or services to us to ensure compliance with this Employee and Supplier Code of Conduct. Ruder Finn and its suppliers shall permit our representative to periodically evaluate your facilities and operations, and those of your subcontractors, to the extent they are providing goods or services to us.



Disability Policy

Ruder Finn will not tolerate unlawful discrimination, harassment, and retaliation in the workplace and off-premises including any work-related settings such as business trips and business-related social functions. In connection with this policy, Ruder Finn expressly prohibits any form of unlawful discrimination, harassment, and retaliation based on characteristics or activities that are protected by law.

Legally protected characteristics include: actual or perceived race (including traits historically associated with race, including but not limited to, hair texture and protective hairstyles such as braids, locks, and twists), color, age, alienage or national origin (including language use restrictions), ancestry, citizenship, religion (including religious dress and grooming practices), sexual orientation, sex or gender (including pregnancy, childbirth, breastfeeding, or related medical conditions), gender identity or gender expression, military or veteran status, disability, genetic information, medical condition (including cancer), or any other characteristic protected by applicable federal, state, or local law.

Legally protected activities include: reporting a complaint or concern with regard to potential violations of this policy, regardless of whether the complaint or concern is raised internally or to a government agency; resisting or opposing practices or conduct that contradicts this policy; participating in an investigation into possible violations of this policy; requesting the use of sick days or other protected time off (such as pregnancy disability leave, and where applicable, family and medical leave); and other activities as may be protected by applicable law.

Improper conduct, including the conduct of visitors, contractors, clients and any interference with the ability of employees to perform their expected job duties is not tolerated.

Recruitment Policy

Ruder Finn is an Equal Opportunity Employer. We are committed to a workplace environment that encourages growth and respect for all current and prospective employees based upon job-related factors such as their educational background, work experience, and ability to perform the essential functions of a particular job.

We invite all applicants to voluntarily self-identify their race, gender, veteran, and disability status. This allows us to collect data on our candidate population and ensure that we have a diverse pool of applicants. It is the policy and practice of Ruder Finn to prohibit any form of discrimination or harassment based on actual or perceived race (including traits historically associated with race, including but not limited to, hair texture and hairstyles such as braids, locks and twists), color, age, citizenship, alienage or national origin, religion, marital status, sexual orientation, sex or gender (including pregnancy, childbirth, breastfeeding or related medical conditions), gender identity or gender expression, military or veteran status, physical or mental disability, genetic information, medical condition (including cancer), or any other status protected under applicable federal, state or local law.

Employee Cyber Security Policy

The purpose of this document is for employees, clients, and prospects to understand the security principals that Ruder Finn Group mandates all employees to follow. These guidelines are brief in nature to allow for easier understanding. More in-depth guidelines can be sought if requested that detail the nuances of managing a complex global cyber security policy. Failure to adhere to these guidelines can result in termination.

Authentication

Authentication is the mechanism of computer systems to verify who the end user is. Any access to Company data or computer systems must require some form of Authentication. Authentication to any Company data will not be granted unless cleared by the Human Resources or Legal department. There are three forms of authentication allowed in the company:

– Password
– Mobile Notification
– Key Exchange

Each computer system and account types must have one or multiple types of Authentications. Authentication methods will be revoked immediately upon termination of services.

Multifactor

All employees, freelancers, and contractors who have access to the Company's data must pass multiple factors (e.g., Multifactor) to be allowed access to data on a device. The two methods which the company supports are Passwords and Mobile Device notification.

Passwords

Passwords are text given to a computer system for validation of the end users. Given the strength of computers being able to automate guessing strong passwords are a necessity. These guidelines will create passwords that are both secure and useable.

Password Construction

The organization mandates that users adhere to the following guidelines on password construction.

– Passwords must be at least 8 characters.
– Passwords must be comprised of a mix of letters, numbers, and special characters.
– Passwords must be comprised of at least one capital and one number and/or symbol.
– Passwords must not be comprised of an obvious keyboard sequence (i.e., qwerty)
– Passwords must not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.
– All passwords for Batch/Service accounts will have a minimum password length of 12 characters.

Password Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords.

– Users must not disclose their passwords to anyone.
– Users must not share their passwords with others (co-workers, supervisors, family, etc.)
– Users must not write down their passwords and leave them unsecured.
– Users must not check the "save password" box when authenticating applications.
– Users must not use the same password for different systems and/or accounts.
– Users must not send passwords via email.
– Users must not re-use passwords for at least 12 password cycles

Password Change Frequency

To maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days. Service account passwords must be changed at least annually.

Password Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to IT. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected of having been compromised IT will request that the user, or users, change all his or her passwords.

Mobile Notification

Mobile phones can be used as a method of authentication, however they cannot be the sole method. Mobile notifications are set up by the Information Technology department at the beginning of engagement with the Company. Notifications will be sent to either the employees' personal or corporate owned device.

Key Exchange

Key exchange is a popular form of authentication to connect to servers mostly through Secure Shell (SSH). Key exchange is a valid means of connecting to a remote server in the company. Key exchange is the process of verifying that the remote user and target system are verified as the expected systems by using the number theory discipline of Mathematics.

Keys must be rotated at least annually or whenever there has been a staffing change.

Key Construction

Keys that are constructed must be no less than 2048 bits of entropy and encoded with the RSA algorithm. They must be secured via passphrase that is no less than 7 characters when used for interactive sessions.

Key Confidentiality

Keys must be kept confidential and not shared among employees. Only Public Keys may be shared for the aid in allowing authorized access.

Key Rotation Frequency

Keys must be rotated for all accounts at least annually or whenever an employee changes status or projects. Key changes will be managed by the IT Department.

Data Management

Once access is given to the Company's systems there must be a set of guidelines in how the information in the Company is handled.

Data Access and Account

During the initial account setup, certain checks must be performed to ensure the integrity of authorization process. The following policies apply to account setup:

– Positive ID and coordination with Human Resources is required.
– Users will be granted the least amount of network access required to perform his or her job function.
– Users will be granted access only if he or she accepts the Acceptable Use Policy.
– Sharing of any passwords is prohibited.
– After five (5) or fewer consecutive unsuccessful logon attempts, the system will initiate controls to limit repetitive "brute force" attempts and suspend the involved end user account after a minimum of 60 minutes.
– Users must be required to change passwords at least every 90 days.
– Accounts which do not automatically enforce password change, reuse, or expiration policies must have a documented plan for changing the password on a periodic basis.

Account Use

User accounts must be implemented in a standard fashion and utilized consistently across the organization. The following guidelines apply to account use:

– Accounts must be created using a standard format.
– User accounts must be protected with multi-factor.
– Accounts must be for individual use only.
– Individuals requiring access to confidential data must have an individual, distinct account. This account may be subjected to monitoring or auditing at the discretion of the IT department or executive team, or as required by applicable regulations or third-party agreements.

Minimum Configuration for Access

Any account connecting to the Company's data must abide by a minimum configuration. This includes devices that have not been jailbroken(rooted) and out-of-date. The company will provide compliant devices to their end users.

Data Storage Locations

The locations of data storage are just as important as access. Storage must be following these guidelines.

Physical Data Storage

All physical data must be encrypted while at rest. This includes laptops, mobile devices, and portable storage devices. All encryption must be no less than 256 bits AES. Additionally, all devices that contain company data must be kept on the employee persons or reside in a secure location. Local access to the data must be protected by

– PIN
– Password
– Biometrics

Cloud Data Storage

Company data must never be uploaded to a non-approved cloud storage location. The Information Technology department maintains the list of acceptable sites and may block certain sites if deemed necessary. The group heads will instruct individual employees about their specific workflows.

Data Transportation

For data to be useful it must be transported from one location to the next. The following are the guidelines for acceptable use thereof.

Physical Data Transportation

When transporting physical data the device must be always encrypted and kept with the person. A chain of custody is required if data is handed off to a third party. In the event of handing the data to a 3rd party the data must be in a locked and encrypted state to prevent unauthorized access. In the event of loss of data during transportation the Information Technology department must be notified immediately.

Digital Data Transportation

When transformation is transferred digitally it must be encrypted. Suitable methods of encryption include such means as TLS (Transport Layer Security), HTTPS, S/MIME and PGP. These methods will be enforced by the Information Technology department.

Data Sharing

Company data must never be shared with any 3rd party unless specifically authorized by Group Head, and Legal, or Information Technology department. This can include such services as Dropbox, WeTransfer, Facebook, Google, etc. Failure to comply can result in termination.

Data Retention Period

The company reserves the right to keep some types of data up to 7 years or longer, if necessary, for regulatory requirements or contractual obligations.

Data Destruction

Data destruction is a necessary part of the data life cycle. Data destruction that an employee feels may be harmful to themselves or to cover up a violation of a law or company policy is strictly prohibited. Data may be destroyed upon written client.

User Accessible Systems

The points of which data is transmitted and received can be a vector of a cyber-attack and must be protected as such.

Endpoints

Endpoints (e.g. Mobile Devices or Computers) are the 'front line' to how the Company operates. All company owned employee endpoints must have the following safeguards in place:

– No Administrator rights for the assigned user
– Anti-virus protection enabled
– Web Filtering Enabled
– Email Filtering Emailed
– Data Management Software
– Standard Software unless otherwise documented and approved by executive management.
– Standard Configuration unless otherwise document and approved by executive management.

Antivirus

All company owned devices have anti-virus installed. The anti-virus solution utilizes a signature-based protection and be heuristic based. The anti-virus cannot be turned off by the end user. The antivirus needs to report to a central authority and notifications of possible intrusions or abnormal behavior must be reported to the Information Technology department.

Filtering

All web traffic is filtered for the prevention of malware and viruses. To this affect all traffic will be sent to a central authority for comparison to know bad actors. Reports will be generated for the Information Technology department for inspection.

Email

All email is subjected to monitoring and filtering for anything that is potentially malicious or against the Company's acceptable use policy. The prohibited items includes:

– Spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes.
– Forging email header information or attempting to impersonate another person.
– Open attachments from unknown senders or when such attachments are unexpected.
– Engage in activity that is illegal under local, state, federal, or international law.
– Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
– Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
– Engage in activities that cause an invasion of privacy.
– Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
– Make fraudulent offers for products or services.
– Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
– Install or distribute unlicensed or "pirated" software.
– Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

Training

All employees will be required to participate in security training annually by the company on the ways that they can help keep data safe. The curriculum will be with real life examples and include a test to ensure that the training principals are internalized.

Updates

Software and to lesser extent hardware are pieces of ever evolving technology and are designed imperfectly. To help mitigate risk software must be updated in a reasonable timeframe once the supplier has made an update available. End user machines shall be updated automatically and forced if passed the period allotted. Infrastructure shall be updated upon approval of the Information Technology department.

Infrastructure and Automation

The autonomous infrastructure that transports data and completes business tasks must adhere to the following provisions.

Automated Alerts

Alerts and automated checks must be in place for all critical infrastructure and tests must be conducted regularly to ensure the alerts are still functioning as intended. Device uptime, last online, communications failure, disk operations, database write failures are all examples of alerts that need to be put into place for a secure environment.

Updates

Updates and critical patches are required to be tested and implemented in a timely manner. Each piece of software must have a documented update channel including checksums and verified authors. Updates once tested will be deployed automatically across all affected devices and verification of successful installation must occur.

Logging

Event logging is paramount for root cause analysis of any abnormal events and will be implemented across all devices. Events that are required to be logged include but not limited, User Sign in events, software execution events, software configuration changes, network configuration changes, network activity, disk write activities, and running processes.

Configuration Baseline

All devices must adhere to a baseline configuration that has a least permissive security stance. The United States Department of Defense Standard Implementation Guidelines (STIG) is used where appropriate in developing the baseline.

Script Execution

All automated scripts and tasks must be documented, and all instances of script execution must be logged and audited.

Continuing Education

Technology never stops evolving and the staff who maintain it must always keep up with the latest practices, standards, and technology through continued education. The workplace must support these endeavors and the financial and time commitment they require.