VeridicaSystems Corporation Comprehensive Anti-Interference Policy

Purpose and Policy Statement

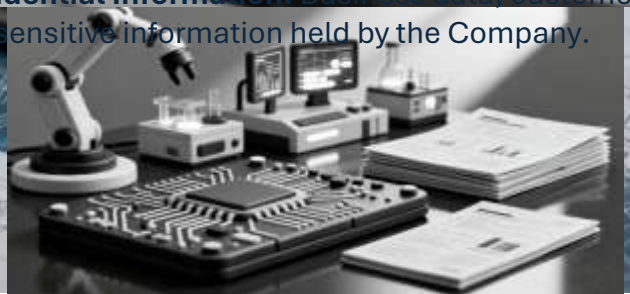
VeridicaSystems Corporation (the **Company**) is committed to protecting all facets of its business operations from unlawful interference. This **Anti-Interference Policy** affirms the Company's right to take **full legal action** – including civil litigation and referral for criminal prosecution – against any individual or entity that "messes with" the Company's operations in any way. The Policy is grounded in robust legal authority at the local, state, federal, and international levels, ensuring it is enforceable and comprehensive. In essence, any act that disrupts or harms the Company's business will trigger swift and aggressive legal remedies available to the Company under applicable law.

Scope of Application

Covered Parties: This Policy applies **universally** to all persons and organizations who interact with the Company. This includes, but is not limited to, all employees, officers, directors, contractors, suppliers, distributors, partners, customers, competitors, and any other external individuals or entities. **The sole exception is the Company's Chief Executive Officer & Founder, John William Dezell**, who is not subject to this Policy's restrictions. Aside from this one exception, no internal or external party is exempt from compliance.

Covered Operations: This Policy is all-encompassing in scope. It covers **all aspects of the Company's operations**, including but not limited to:

- **Contracts and Business Relationships:** Formation, performance, and enforcement of contracts with employees, clients, vendors, and partners.
- **Supply Chain and Logistics:** Procurement processes, supplier dealings, product manufacturing, and delivery systems.
- **Intellectual Property (IP):** The Company's patents, trademarks, copyrights, trade secrets, and proprietary information.
- **Finances and Assets:** Financial systems, accounts, investments, and Company property (funds, equipment, facilities).
- **Digital Infrastructure:** Information systems, networks, software, databases, and cybersecurity mechanisms.
- **Personnel and Workplace:** Company employees, management, and contractors, including workplace security and safety.
- **Data and Confidential Information:** Business data, customer data, and any confidential or sensitive information held by the Company.



- **Customer Relationships:** Interactions with customers, client accounts, sales relationships, and customer data/privacy.
- **Regulatory Compliance:** The Company's adherence to laws and regulations, licenses, permits, and engagement with regulators.
- **Communications:** Corporate communications, whether internal (emails, reports) or external (marketing, press, public statements).
- **Corporate Governance:** The functioning of the Company's board of directors, shareholder rights, corporate records, and decision-making processes.

In every context listed above, this Policy ensures that any interference or harm will be met with appropriate legal action. The Policy may be referenced in internal governance documents, included as protective clauses in contracts, incorporated into employee and contractor agreements, and invoked in legal filings or public statements, thereby providing a consistent protective stance across all business activities.

Definition of "Messed With" (Prohibited Interference)

For purposes of this Policy, **"messed with"** is defined as any **intentional or negligent act or omission** by any person or entity (other than the CEO as noted) that disrupts, harms, or otherwise **interferes with the Company's operations or interests**. This broad definition of interference includes, **but is not limited to**, the following forms of misconduct:

- **Disruption of Business Processes:** Any act that **impedes or interrupts** the Company's normal business activities, services, or supply chains – whether through deliberate meddling or careless conduct. This covers interference with contract performance, preventing the Company from fulfilling its obligations or enjoying its rights in a business relationship (a harm actionable under tort law)[1][2].
- **Sabotage:** Any **deliberate damage or destruction** aimed at the Company's operations, assets, or reputation. Sabotage can be physical (e.g. vandalizing facilities or equipment) or digital (e.g. introducing malware). It encompasses **industrial sabotage** in any form, such as tampering with products, disrupting supply deliveries, or impairing the function of the Company's systems. Such acts may violate criminal laws against property damage (e.g. Pennsylvania's criminal mischief statutes) and even federal laws if interstate commerce is affected or if done as part of a broader criminal scheme (potentially implicating racketeering laws).
- **Fraud and Deceit:** Any **fraudulent behavior** targeting the Company, including misrepresentation, false pretenses, or deceptive schemes that cause the Company harm. This includes fraud by vendors, customers, or even insiders, such as falsifying records, diverting funds, or engaging in **contractual fraud**. Under Pennsylvania and U.S. law, fraud against a business can lead to civil liability and criminal charges (for example, mail or wire fraud under federal law, which are crimes to scheme and defraud a company of its property)[3]. Fraud that interferes with the Company's rights or property may also serve as a predicate act under the

federal Racketeer Influenced and Corrupt Organizations Act (RICO) (see **Legal Foundations** below)[4][5].

- **Breach of Confidentiality:** Any **unauthorized disclosure or misuse of the Company's confidential information**. This includes breaking non-disclosure agreements (NDAs), leaking trade secrets, or otherwise failing to protect proprietary data. Even negligently handling sensitive data (leading to a leak) falls under "messed with." The Pennsylvania Uniform Trade Secrets Act (PUTSA) specifically prohibits the misappropriation of trade secrets, defining "improper means" to obtain secrets as including theft, bribery, **breach or inducement of a breach of a duty to maintain secrecy**, or espionage[6]. In short, anyone who steals or divulges the Company's confidential business information – whether an ex-employee, a competitor, or a hacker – is interfering with the Company and will face legal action.
- **Tampering:** Any **alteration, manipulation, or unauthorized access** involving the Company's systems, products, or records. Tampering includes manipulating financial books, altering digital data without permission, physically tinkering with equipment, or corrupting product quality. For example, tampering with the Company's digital infrastructure or data may violate state computer crime laws (Pennsylvania law criminalizes unauthorized alteration or destruction of computer data/programs)[7]. Likewise, tampering with physical products or safety systems could invoke criminal product tampering statutes and tort liability for any damages caused.
- **Theft and Property Misappropriation:** Any form of **theft, embezzlement, or misappropriation** of the Company's property – whether tangible assets, funds, or intellectual property. This includes stealing equipment or inventory, diverting Company funds, or stealing data/IP (such as copying software, client lists, or research without authorization). Theft of trade secrets is both a state-law violation under PUTSA and a federal crime under the Economic Espionage Act (18 U.S.C. § 1832). The Company will pursue civil damages and criminal remedies for any theft. Even unauthorized accessing of Company computer systems to obtain information is unlawful (Pennsylvania's **Computer Theft** statute, 18 Pa.C.S. § 7613, makes it a felony to use a computer to steal data or files)[8].
- **Defamation and Disparagement:** Any **false statements** made about the Company, its products, or its personnel that harm the Company's reputation or business relationships. This includes slander (spoken defamation), libel (written defamation), and **commercial disparagement** (false statements about the quality or legitimacy of the Company's goods or services). Pennsylvania law provides a remedy to businesses for disparagement of their products or services by others[9]. For example, a person or competitor who spreads false rumors that the Company's product is unsafe or that the Company engages in fraud is "messing with" the Company's customer relationships and goodwill. Such conduct is actionable as commercial disparagement or business defamation, requiring the offender to pay damages if the falsehood caused financial loss[10]. Defamatory interference with

the Company's relationships will prompt legal action for injunctive relief and damages against the speaker.

- **Obstruction and Coercion:** Any **obstruction of the Company's activities or coercion upon the Company or its staff**. Obstruction includes blocking or hindering the Company's **business operations or legal rights** – for instance, interfering with a contractual negotiation or sabotaging a regulatory approval process. It also includes attempts to **obstruct justice or regulatory compliance**, such as destroying records or providing false information to regulators to cause the Company trouble. Coercion involves **threats, blackmail, or extortion** against the Company or its employees to force some action (or inaction) that harms the Company. Such conduct often violates criminal laws – e.g. Pennsylvania's laws against intimidation and extortion, and federal laws like the Hobbs Act (18 U.S.C. § 1951) which makes it a crime to obstruct or affect commerce by threats, violence or extortion[11]. Any attempt to strong-arm the Company (for example, threats to reveal sensitive data unless the Company pays money) will be met with immediate legal action and involvement of law enforcement.
- **Cyberattacks and Digital Intrusions:** Any **cyberattack, hacking, or unauthorized interference** with the Company's computers, networks, or data. This includes attempts to gain unauthorized access to systems, deployment of viruses or malware, denial-of-service (DoS) attacks, ransomware incidents, phishing campaigns targeting the Company, or any **cyber intrusion** whatsoever. Such acts are explicitly illegal under multiple laws. For example, the U.S. Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030) is a key federal law used to prosecute cybercrimes and unauthorized computer access[12]. Pennsylvania law similarly criminalizes hacking and related offenses: **Unlawful Use of a Computer** (18 Pa.C.S. § 7611) makes it a felony to access any computer or data without authorization[13], and related provisions outlaw causing network malfunctions, computer trespass, and virus distribution[7]. Under this Policy, any cyberattack on the Company is considered a direct attack on our "digital infrastructure" and will trigger legal action. The Company will work with law enforcement (local, state, federal, and international as needed) to prosecute cybercriminals to the fullest extent (including invoking international cybercrime treaties as described below).
- **Other Forms of Interference:** The above categories are illustrative but not exhaustive. **Any other form of intentional wrongdoing or grossly negligent act that interferes with the Company's operations, rights, or interests is prohibited.** This catch-all includes things like: bribing or influencing third parties to the Company's detriment (for instance, inducing a supplier to breach its contract), organizing boycotts or blockades through unlawful means, misusing the Company's intellectual property (trademark or copyright infringement can be viewed as interference with IP assets), or interfering with corporate governance (e.g. a stockholder or outsider engaging in **coercive or fraudulent tactics in a corporate vote or decision-making process**). All such acts – essentially, anything that

**"messing with the Company" could colloquially encompass – fall under this Policy and will face legal challenge.

Note: This Policy covers interference whether it is **intentional, knowing, reckless, or negligent**. While many of the acts described imply deliberate misconduct, even a failure to follow required duties (negligence) that results in serious disruption to the Company may lead to action under this Policy (particularly if contractual or fiduciary duties are breached). The overriding principle is that **the Company's operations are sacrosanct**, and any wrongful interference, by act or omission, will be met with legal recourse.

Legal Foundations and Applicable Law

VeridicaSystems anchors this Policy in a strong legal framework spanning **local Pennsylvania ordinances, Pennsylvania state law, U.S. federal law, and international legal regimes**. The Company's right to take action against interference is supported at **every level of law**. The following is an overview of key legal authorities and how they correspond to the types of "messing with" described above:

Pennsylvania Law (Local and Commonwealth)

Local Ordinances: In the municipalities where the Company operates (within Pennsylvania), local laws and ordinances provide basic protections against interference. For example, local ordinances and police enforcement address **trespassing, disorderly conduct, vandalism, and harassment** that could disrupt a business. If an individual trespasses on Company property or causes a disturbance at a Company facility, local law enforcement can issue citations or make arrests under applicable city codes. (E.g., in Pennsylvania, **criminal trespass** is unlawful under 18 Pa.C.S. § 3503: a person commits an offense if, knowing he is not licensed or privileged, he enters or remains in any place where notice against trespass was given[14].) Such local measures complement state law: the Company will invoke **police assistance and local legal remedies immediately** for on-site interference or any breach of the peace affecting its operations.

Pennsylvania Criminal Law: The Pennsylvania Crimes Code provides numerous tools to address someone interfering with the Company. Relevant Pennsylvania criminal statutes include:

- **Criminal Trespass (18 Pa.C.S. § 3503):** Unlawful entry onto Company premises (or remaining after being told to leave) is a criminal offense[14]. This protects the Company's facilities and offices from intruders or protestors who might disrupt operations.
- **Criminal Mischief (18 Pa.C.S. § 3304):** This statute makes it a crime to **damage or tamper with property**. Anyone who vandalizes Company property, equipment, or data storage (e.g. physically damaging computers or defacing buildings) can be prosecuted. Sabotaging equipment or products would fall under this provision.
- **Pennsylvania Cybercrime Statutes:** Pennsylvania has a robust set of computer crime laws to combat digital interference. These include: **Unlawful Use of**

Computer (18 Pa.C.S. § 7611) – broadly criminalizing unauthorized access or use of computer systems[13]; **Disruption of Service (18 Pa.C.S. § 7612)** – criminalizing denial-of-service or other acts that disrupt computer services[7]; **Computer Theft (18 Pa.C.S. § 7613)** – making it a felony to use a computer to steal information or data[8]; **Unlawful Duplication (18 Pa.C.S. § 7614)** – criminalizing copying of data/software without authorization[15]; **Computer Trespass (18 Pa.C.S. § 7615)** – covering unauthorized removal or alteration of data and other intrusions[16]; and **Distribution of Malware (18 Pa.C.S. § 7616)** – outlawing the distribution of computer viruses[7]. In short, Pennsylvania law treats hacking, electronic sabotage, and data theft as serious felonies, empowering the Company to seek prosecution of hackers or rogue insiders under state law.

- **Theft and Fraud Offenses:** Pennsylvania law criminalizes theft (unlawful taking of property or services) and fraud (deception to cause loss). If anyone steals Company property (equipment, funds, or trade secrets) or commits fraud against the Company (such as a vendor submitting fake invoices or an employee embezzling money), they can face charges like **Theft by Unlawful Taking, Theft by Deception, Forgery, Securing Execution of Documents by Deception**, and related offenses in the Pennsylvania Code. Notably, Pennsylvania also has a statute for **"Theft of Trade Secrets"** (18 Pa.C.S. § 3930) which specifically penalizes the theft of confidential business information. These laws reinforce that those who misappropriate Company assets will be subject to criminal sanction.
- **Extortion and Coercion:** If a person attempts to extort the Company (e.g. "pay me or I'll harm your business"), Pennsylvania law can charge them with crimes like **Theft by Extortion** or **Criminal Coercion**. Pennsylvania's **terroristic threats** statute (18 Pa.C.S. § 2706) also makes it a crime to threaten unlawful violence intending to cause terror or public inconvenience – which could apply if someone threatens the Company's employees or facilities to disrupt operations.
- **Defamation and Commercial Disparagement:** While defamation is generally a civil matter, Pennsylvania recognizes a business's legal right to be free from malicious falsehoods. The **Pennsylvania Unfair Trade Practices and Consumer Protection Law** forbids disparaging another's goods, services, or business with false or misleading statements (73 P.S. § 201-2(4)(viii)), reflecting a public policy against business defamation[17]. Additionally, any coordinated campaign of falsehoods meant to sabotage the Company's market standing could potentially be scrutinized under criminal statutes (for instance, criminal conspiracy if multiple parties collude to spread injurious lies). Primarily, however, the Company will use civil litigation to address defamation (see below), while reserving the right to involve authorities if the conduct edges into fraud or harassment.

Pennsylvania Civil Law: The Company also has powerful civil remedies under Pennsylvania law to hold wrongdoers accountable financially and halt interference:

- **Tortious Interference:** Pennsylvania common law recognizes the tort of **Intentional Interference with Contractual or Business Relations**. In

Pennsylvania, one who **intentionally and improperly interferes** with the performance of a contract or with another's business relationships can be held liable for the harm caused[1]. For example, if a competitor induces one of the Company's clients to break a contract, or if a former employee tries to lure away an entire team of our employees in violation of non-solicitation agreements, the Company can sue for tortious interference. To prevail, the Company would show: (1) a contractual or prospective economic relationship existed, (2) the defendant acted with the purpose of harming that relationship, (3) without privilege or justification, (4) causing actual damage[2]. This Policy makes clear that any such interference with our contracts or customer relationships will lead to such a lawsuit. Pennsylvania courts have long upheld this cause of action to protect businesses from outsiders who would sabotage their dealings[1][2].

- **Pennsylvania Uniform Trade Secrets Act (PUTSA):** As noted, trade secret theft falls under PUTSA (12 Pa. Cons. Stat. § 5301 et seq.). Under PUTSA, the Company can bring a civil lawsuit against anyone who misappropriates its trade secrets by improper means[6]. Remedies include **injunctions** to stop further use or disclosure of the secret, **damages** for economic loss, and in cases of willful misconduct, **punitive damages and attorney's fees**. PUTSA's definitions explicitly cover breaches of confidentiality and electronic espionage[6], aligning with this Policy's prohibition on data theft and leaks. This Policy will be referenced in all Company NDAs and confidentiality agreements to underscore that we will enforce our trade secret rights vigorously under PUTSA and related laws.
- **Defamation/Commercial Disparagement (Civil):** If a person or entity disseminates false statements that damage the Company, the Company can file a civil suit for defamation or, in the business context, **commercial disparagement**. Pennsylvania law provides that a business has a viable claim if someone publishes a false statement about the business or its products knowing (or having reason to know) it will cause financial harm and if harm results[9][10]. The Company would seek monetary damages for lost profits and reputational harm, as well as possible injunctive relief to stop further false statements. This Policy's broad definition of "messed with" to include defamation ensures that those who smear the Company's name will face legal consequences.
- **Breach of Contract and Fiduciary Duty:** Internal interference by employees, officers, or business partners will often give rise to breach of contract claims or breach of fiduciary duty. For instance, an employee who "takes company data" or disrupts operations might be breaching their employment contract or confidentiality agreement – the Company will sue for any such breach. Similarly, a disloyal executive who undermines the Company could be sued for breaching fiduciary duties. While the Policy excepts the CEO from its scope, all other officers and agents are fully accountable. The Policy language can be integrated into contracts (employment contracts, contractor agreements, partnership agreements) to explicitly make such interference a material breach, streamlining the Company's right to injunctive relief and damages in court.

- **Equitable Remedies:** In Pennsylvania courts, the Company can seek **injunctions** (court orders) to immediately stop ongoing interference. Because many interferences (like trade secret theft, defamation, or sabotage) cause irreparable harm, courts may grant temporary restraining orders and preliminary injunctions to halt the wrongful conduct. For example, under PUTSA, a court can enjoin actual or threatened misappropriation of trade secrets[18]. Likewise, for breach of a non-compete or a confidentiality agreement, injunctive relief is often available. This Policy explicitly contemplates the use of such legal tools to **swiftly end any interference** before damage mounts.

In summary, Pennsylvania's legal system (both criminal and civil) is well-equipped to back this Policy. The Company will not hesitate to coordinate with **Pennsylvania law enforcement** to press criminal charges when a law is broken, or to file lawsuits in Pennsylvania courts to obtain damages and injunctions. All personnel and partners of the Company are put on notice by this Policy that Pennsylvania law is on the Company's side to punish any acts of interference.

United States Federal Law

At the federal level, a wide array of laws protect businesses from interference, and VeridicaSystems will invoke these where applicable. Federal law is especially crucial for addressing **interstate or complex schemes** of interference, cyber incidents that cross state or national borders, and sophisticated forms of corporate sabotage. Key federal legal frameworks include:

Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030: The CFAA is the primary federal anti-hacking statute and a cornerstone of cybersecurity law. It broadly prohibits unauthorized access to protected computers, theft of information via computer, spreading malware, and related online crimes. In the Department of Justice's own words, the CFAA "is an important law for prosecutors to address cyber-based crimes"[12]. Under the CFAA, it is a federal offense to intentionally access a computer without authorization (or in excess of authorization) and obtain information, cause damage, or further a fraud[19][20]. It also criminalizes knowing transmission of malware that causes damage and any extortionate threats involving computers (such as ransomware schemes)[21][22]. The Company will refer serious cyberattacks to federal authorities under the CFAA. The CFAA also provides for a civil cause of action in some cases, meaning the Company could sue the perpetrator for compensatory damages and injunctions in federal court. This Policy aligns with CFAA by treating cyber "messing with" (hacking, data theft, DoS attacks, etc.) as grave offenses. We will leverage federal resources (FBI, Secret Service, etc.) and legal remedies under CFAA for any significant cyber incident that impacts the Company's systems or data.

Electronic Communications Privacy Act (ECPA) and Related Laws: ECPA (which includes the Stored Communications Act) prohibits unauthorized interception of electronic communications and unauthorized access to stored electronic communications. If an individual were to wiretap the Company's communications or hack

into email servers, that triggers ECPA. Other federal laws protect against specific tech harms (for example, the **Digital Millennium Copyright Act** has anti-circumvention provisions that might apply if someone tampers with the Company's digital rights management). While too numerous to list exhaustively, the presence of these laws means **digital interference and spying** on the Company can be met with federal prosecution or civil suits. The Company's Policy therefore finds support in these statutes for any invasions of our electronic privacy or integrity.

Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1836: In addition to state trade secret law (PUTSA), the Company can invoke the federal DTSA. Enacted in 2016, DTSA created a federal civil action for trade secret misappropriation, allowing companies to sue in federal court for theft of trade secrets. It largely parallels PUTSA in substance (e.g., allowing injunctions, damages, and even seizure orders in extraordinary cases), but is important if the misappropriation is interstate or involves foreign actors. If, for example, an employee takes trade secrets and moves to another state, or a foreign competitor hacks our servers for proprietary data, DTSA provides a federal forum to pursue them. The **Economic Espionage Act (EEA), 18 U.S.C. §§ 1831-1832**, is the criminal counterpart that makes trade secret theft a federal crime (with enhanced penalties if done for the benefit of a foreign government or entity). While the EEA's trade-secret theft provision is not itself a RICO predicate[3], the theft often involves **mail or wire fraud**, which *are* RICO predicates as explained below. Under this Policy, any cross-border or interstate theft of our secrets will prompt us to utilize DTSA (civilly) and refer matters to the DOJ under the EEA (criminally).

Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961–1968: RICO is a powerful federal law originally designed to combat organized crime, but it also provides a **civil cause of action** for businesses harmed by a pattern of criminal activity. In short, if an individual or group engages in a **pattern of racketeering activity** (meaning at least two specified criminal acts within 10 years) that injures the Company's business or property, the Company can sue under civil RICO. Importantly, **RICO permits a company that has been victimized by criminal conduct to bring a civil lawsuit against the perpetrator**[4]. The advantages for the Company include access to federal courts, recovery of **treble damages (three times the actual damages)** and **attorney's fees**, and the fact that a RICO judgment (since it's based on egregious fraud) cannot be discharged in bankruptcy[5]. Under RICO, many forms of "messing with" the Company could qualify as racketeering acts – for example, extortion, fraud, theft of corporate funds, and interstate theft of confidential information (via the mail/wire fraud predicates). A notable case upheld a civil RICO claim against a former employee who stole trade secret drawings[4]. If the Company experiences a coordinated campaign of sabotage or fraud (say, a group of conspirators repeatedly hacking us or defrauding us), we will evaluate RICO as an option. The mere threat of treble damages under RICO is a significant deterrent to would-be saboteurs. This Policy explicitly aligns with RICO: any **pattern of criminal interference** with the Company (two or more related acts, like repeated hacking or serial acts of fraud) will lead us to consider RICO charges in addition to individual criminal charges. We will not hesitate to use "the big stick" of RICO litigation to protect the Company's interests[4][5].

Federal Criminal Law – Fraud, Extortion, etc.: The U.S. criminal code provides many specific offenses that may apply to interference scenarios, beyond cyber and trade secrets already discussed. For instance:

- **Mail and Wire Fraud (18 U.S.C. §§ 1341, 1343):** If someone engages in a scheme to defraud the Company (or to obtain money/property from the Company) using mail or electronic communications, it's a federal crime. These statutes have broad application; for example, if a person sends false electronic instructions to divert Company funds, or emails lies to our customers to steal business, that could be wire fraud. Notably, as referenced above, the U.S. Supreme Court has held that **confidential business information** is "property" protected by these fraud statutes[23]. Thus, scheming to steal the Company's confidential data via email can be prosecuted as wire fraud[23]. The Company will involve federal law enforcement for any significant fraud or deception that crosses state lines or uses national communication channels.
- **Interstate Threats and Extortion (Hobbs Act, 18 U.S.C. § 1951):** The **Hobbs Act** makes it a federal crime to obstruct or affect interstate commerce by **robbery or extortion**. Extortion is defined as obtaining property via wrongful use of force, violence, or **fear** (including fear of economic harm)[11][24]. If a malicious actor threatens the Company (for example, "Give me a job or I'll leak your trade secrets" or "Pay us or we'll disrupt your supply shipments"), and that threat could affect commerce, the FBI can pursue it under the Hobbs Act. This Policy's coverage of coercion and extortion is firmly supported by such federal law – any extortion attempt will be treated as a federal offense. Additionally, sending threats across state lines (18 U.S.C. § 875) or threatening communications in interstate commerce (which can include cyber-extortion threats) are separate federal crimes. In sum, the Company can call upon federal prosecutors for any scenario where threats or coercion are used to "mess with" our business.
- **Federal Intellectual Property (IP) Laws:** Interference with the Company's IP rights (such as trademark infringement, copyright piracy, or patent violations) will be addressed under the respective federal statutes. For example, if a competitor copies our software (copyright infringement) or uses a confusingly similar brand name (trademark infringement), those are violations of the Copyright Act (17 U.S.C.) or Lanham Act (15 U.S.C. §§ 1114, 1125) and we will sue in federal court. While such IP infringements are not typically seen as "sabotage" in the traditional sense, they **do interfere** with our business and are therefore covered by this Policy. In serious cases (like willful commercial piracy or counterfeiting), criminal enforcement is possible (e.g., criminal copyright infringement, 17 U.S.C. § 506, or trafficking in counterfeit goods, 18 U.S.C. § 2320). The Policy's reference to IP in its scope is backed by these laws to ensure our exclusive rights are protected globally.
- **Securities and Corporate Fraud:** If VeridicaSystems were to be a publicly reporting company or have shareholders, federal laws (e.g., SEC regulations, Sarbanes-Oxley Act provisions against corporate fraud and record tampering) would offer additional protection. Any attempt to interfere with our corporate governance through deceit

(such as falsifying SEC filings or bribing auditors) would violate federal securities laws and Sarbanes-Oxley (18 U.S.C. § 1519 makes it a crime to destroy or falsify corporate records to obstruct an investigation). While the specifics depend on the Company's status, this Policy would be enforceable via those federal channels if needed, ensuring our corporate governance cannot be undermined without legal repercussions.

Overall, the federal legal framework significantly bolsters this Policy. It allows the Company to pursue offenders across state lines, seek harsher penalties for organized or repeated attacks, and leverage federal investigative agencies for complex cases (like international hackers or multi-state fraud rings). By citing these federal laws in our contracts and policies, we put all parties on notice that **any interference could escalate to a federal case**. The Company is prepared to cooperate with federal authorities (FBI, U.S. Secret Service, Homeland Security, etc.) and invoke federal jurisdiction whenever interference with our business transcends Pennsylvania or involves specialized federal concerns (cybersecurity, racketeering, IP theft, etc.).

International Legal Frameworks

VeridicaSystems operates in a global environment and enjoys protection under **international law and treaties** that address cross-border interference, intellectual property rights, and cybercrime. We align this Policy with applicable international frameworks to ensure that our rights are respected and enforceable worldwide:

Intellectual Property Treaties: The Company's intellectual property is safeguarded not only by U.S. law but also by international agreements that harmonize and enforce IP rights across borders. Notably, the **Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)**, administered by the World Trade Organization, requires all member countries (including the U.S. and virtually all major economies) to uphold strong IP protection and enforcement measures[25][26]. TRIPS establishes minimum standards for protecting patents, trademarks, copyrights, trade secrets, and more, and crucially obligates countries to provide foreign IP owners the **same legal protection as domestic owners**[26]. This means if the Company's IP is "messed with" in a foreign country (e.g. a foreign entity infringes our patent or steals our trade secrets), we can expect legal recourse in that country's courts comparable to what a local company would get, thanks to TRIPS. Additionally, treaties like the **Paris Convention** (for patents and trademarks) and the **Berne Convention** (for copyrights) simplify cross-border recognition of IP rights. For example, the Paris Convention lets us use our U.S. patent filing date in member countries, preventing others from stealing a march on our inventions abroad[27][28]. The Berne Convention ensures our copyrighted software or documentation is automatically protected in all member countries without local registration[29][30]. In summary, international IP treaties form a web of protection so that interference with our IP (like counterfeiting our products or pirating our software in another country) can be fought through coordinated legal action internationally. The Company will leverage these treaties by registering its IP in key jurisdictions and collaborating with foreign counsel and law

enforcement to stop cross-border IP violations. If someone halfway around the world "messes with" our trademarks or steals our trade secrets, treaty obligations (including various anti-counterfeiting trade agreements) will help us hold them accountable in that jurisdiction.

International Cybercrime Cooperation: Cyber threats are often transnational – an attacker might reside outside the U.S. Therefore, this Policy is reinforced by global cybercrime treaties that facilitate international law enforcement collaboration. Chief among these is the **Council of Europe's Convention on Cybercrime (Budapest Convention)**, to which the United States is a party. The Cybercrime Convention is the **first multilateral treaty to specifically address computer-related crime**, requiring signatory nations to criminalize hacking, network interference, and similar acts, and to assist each other in cybercrime investigations[31][32]. Under this framework, if a foreign hacker attacks VeridicaSystems' network, U.S. authorities can request investigative assistance from the hacker's home country (and vice versa), ensuring there are no safe havens for cybercriminals[33][34]. The Convention mandates broad **international cooperation** – from sharing electronic evidence to extraditing cyber offenders[35][34]. Likewise, in 2024 the United Nations adopted a new **U.N. Convention on Cybercrime**, further bolstering global efforts (the U.S. has been actively involved in its development). What this means for the Company is that a cyberattack originating overseas is not beyond reach: through treaties, our government can pursue the perpetrator with the aid of foreign authorities. This Policy explicitly cites cyberattacks as actionable, and we will use instruments like Mutual Legal Assistance Treaties (MLATs) and the Cybercrime Convention to have foreign-based interferers investigated, arrested, and prosecuted.

Cross-Border Law Enforcement and Extradition: In cases of serious interference (fraud, embezzlement, IP theft) where the culprit flees the country or is based abroad, the Company will rely on extradition treaties and international arrest warrants. The U.S. has extradition agreements with numerous countries for crimes like fraud, hacking, and racketeering. For example, if a former employee absconds to another country with trade secrets or funds, many nations will honor a U.S. extradition request to return that person to face charges. Our Policy's threat of "full legal action" truly has global reach – potential wrongdoers cannot evade responsibility by crossing borders.

International Regulatory Compliance: The Policy also ensures we can defend against interference in regulatory contexts internationally. If we are operating or seeking licenses in other countries, local laws (which often echo international standards or treaties) will be invoked. For instance, if a local competitor in a foreign country spreads false information to block our market entry, there may be remedies under that country's unfair competition laws (many of which implement principles from treaties or international models). The Company is prepared to use foreign counsel and international arbitration where needed to address interference abroad, referencing this Policy's principles of zero-tolerance.

Treaty Obligations and Public Policy: By aligning with international legal frameworks, this Policy not only protects the Company but also signals our compliance with global norms.

For example, our commitment to pursue anyone who tampers with data aligns with international norms like the **OECD Guidelines for Security of Information Systems** and reinforces that we take cybersecurity seriously. Similarly, our intolerance of bribery or coercion aligns with the **U.N. Convention Against Corruption**, which many countries follow. Thus, the Policy can be communicated to foreign partners and authorities as being in harmony with international law, aiding its acceptance and enforcement globally.

In summary, **no matter where interference originates or occurs, the Company will find a legal avenue to respond**. Through international IP protections, cross-border law enforcement cooperation, and treaty-based legal rights, VeridicaSystems ensures this Policy's enforceability worldwide. Those who target our business from abroad will face not only U.S. federal action but also the prospect of international prosecution or civil liability in their own countries. This comprehensive, border-neutral approach is a core strength of the Policy.

Enforcement, Implementation, and Usage

This Policy is designed to be **highly versatile** and **integrated into all facets of the Company's protective measures**. Below is how the Policy is enforced and utilized across various contexts of the Company's operations:

Internal Governance Documents: The principles of this Policy will be incorporated into the Company's internal bylaws, codes of conduct, and corporate governance policies. For instance, the Company's Code of Ethics will explicitly forbid any officer, director, or employee from engaging in conduct that "messes with" the Company's operations, with reference to the comprehensive definition herein. The Policy serves as a guiding charter that the Board of Directors can rely on to take action (such as terminating an officer or disciplining an employee) if they engage in interference. While John W. Dezell, the CEO, is exempt from this Policy's *restrictions*, the Policy still provides a framework for how the Company (under his leadership) will respond to interference by others. The Board may also include in corporate resolutions that the Company shall pursue legal remedies against interference aggressively, citing this Policy as the rationale. This ensures that at the highest level, there is institutional commitment to enforcement.

Employee and Contractor Agreements: All employment contracts, independent contractor agreements, and consulting agreements will **reference this Policy or incorporate its substance**. For example, employment agreements will have clauses such as: *"The employee shall not interfere with or disrupt any aspect of the Company's business operations, and shall not engage in any act that falls under the Company's Anti-Interference Policy. Any such conduct will constitute gross misconduct and a material breach of this agreement, subjecting the employee to immediate termination and potential legal action."* Similarly, confidentiality and invention assignment agreements will reiterate that any breach (like misusing confidential info) triggers the Company's right to injunctive relief and damages as per this Policy. For contractors, we will include covenants not to harm the Company's business or reputation and to comply with all security protocols,

backed by the same enforcement rights. By signing these contracts, individuals explicitly acknowledge the Company's right to seek full legal recourse against them for any interference. This not only deters wrongdoing but also puts us in a strong position to get **injunctions or restraining orders** if needed (since the contractual agreement to the Policy can be shown to a court as evidence of the known obligation and risk of harm).

Third-Party Contracts and Clauses: When dealing with suppliers, distributors, joint venture partners, or other business associates, the Company will often insert a **"Non-Interference" clause** in the contract. Such a clause will mirror this Policy's language, stating that the other party agrees not to engage in any activities that could disrupt or harm our operations (e.g., not to poach our employees, not to sabotage deliveries, not to disparage our products, etc.). It will also stipulate that if they do, we have rights to terminate the contract and seek legal remedies. For example, a supply contract may say: *"Supplier shall refrain from any actions that interfere with Buyer's business, including disruption of supply, misuse of Buyer's data, or disparagement of Buyer. In the event of such interference, Buyer may terminate this agreement effective immediately and pursue all remedies available at law or equity."* Embedding the Policy in this way ensures that in any dispute, we can point to contractual breach in addition to underlying legal violations. It makes our case stronger in court and may allow recovering attorneys' fees if the contract specifies. Also, by making it part of the deal, the other party is put on formal notice to behave accordingly.

Legal Filings and Litigation Strategy: Whenever the Company initiates legal action (civil lawsuits or criminal complaints) in response to interference, this Policy provides a **roadmap for our legal team**. The comprehensive definition of prohibited acts helps attorneys identify all possible causes of action. For instance, if an incident occurs (say an ex-employee hacks our system and steals data), our lawyers will consult the Policy and likely file a multi-pronged lawsuit: alleging violations of the Computer Fraud and Abuse Act, the Defend Trade Secrets Act, breach of contract, and so on – reflecting each category in the Policy. We will cite the specific laws referenced in this Policy within our pleadings (e.g., referencing 18 Pa.C.S. § 7611 in a complaint to emphasize the illegality of the hack under state law, or quoting the elements of tortious interference to support a claim). By aligning our litigation with this Policy, we ensure consistency and thoroughness. Courts may also appreciate that the Company had a clear internal policy against the misconduct, which can reinforce our position that the defendant knew or should have known their acts were wrongful (potentially aiding in claims of willfulness or malice, which can affect damages). Moreover, in public-facing legal filings (like a press release about filing suit), we can invoke this Policy to signal to stakeholders and other would-be offenders that we take interference seriously and have a unified legal approach to combat it.

Enforcement Mechanisms: The Company will utilize every legal remedy at its disposal to enforce this Policy:

- **Injunctions and Restraining Orders:** Given the often urgent nature of interference (e.g., a data breach or an ongoing disparagement campaign), seeking immediate

court orders to stop the harmful conduct is a priority. Our legal counsel will be prepared to go into court on short notice to obtain temporary restraining orders (TROs) and preliminary injunctions. The documentation of harm and risk in this Policy can support the "irreparable harm" showing for an injunction. For example, if an ex-employee is about to publish our trade secrets, we will swiftly move for an injunction citing PUTSA[18] to bar that publication. Courts have authority under various statutes to grant such relief (including seizing stolen data or enjoining defamatory publications). This rapid response capability minimizes damage and demonstrates the Policy's teeth.

- **Damages and Recovery:** On the civil side, the Company will seek **monetary damages** to make itself whole and to penalize the offender. As outlined, many laws allow enhanced damages: treble damages under RICO[5], punitive damages under trade secret law for willful misappropriation, statutory damages for willful IP infringement, etc. We will aggressively pursue the maximum damages allowed, partly to deter others. Additionally, we will seek to recover costs and attorneys' fees whenever statutes or contracts permit (for example, RICO provides for attorneys' fees[5], and contracts can stipulate fee-shifting for enforcement). By doing so, we ensure that interfering with VeridicaSystems is economically unviable for any rational actor.
- **Criminal Prosecution:** On the criminal side, while the Company itself cannot press charges, we will promptly involve law enforcement and push for criminal investigation/prosecution of offenders. This means reporting crimes to local police, the Pennsylvania Attorney General's office (e.g., for complex economic crimes or cybercrimes within PA), the FBI or Secret Service for cyber intrusions or interstate schemes, and so forth. We will cooperate as a victim with prosecutors, providing evidence and impact statements. The Policy's catalog of potential crimes (trespass, hacking, extortion, etc.) will guide us in communicating to authorities exactly what laws were broken. Our stance is uncompromising: we will advocate for perpetrators to face the **full extent of criminal penalties** – be it fines, restitution to the Company, or imprisonment. In appropriate cases, we may also pursue parallel civil and criminal actions (for instance, suing for damages while a criminal case proceeds, as both can often occur concurrently).
- **Internal Disciplinary Action:** If the interference comes from an insider (employee or executive), in addition to external legal action, the Company will take swift internal action. This includes immediate termination for cause, removal from position, and, where applicable, reporting licensed professionals to regulatory boards (for example, if a CPA employee commits fraud, reporting them to accountancy boards). The Policy makes it clear that no one within the Company has immunity (aside from the specified CEO exception) – any other person will face not just firing but also potential lawsuits from us. Our employment manuals will refer to this Policy as a basis for disciplinary proceedings.
- **Insurance and Recovery:** The Company carries certain insurance (such as cyber insurance, crime insurance, liability insurance) to mitigate losses from interference.

Enforcing this Policy works hand-in-hand with insurance; for example, our insurers may require us to have a plan to pursue wrongdoers. Proceeds from legal actions (damages awards or restitution) will be used, where required, to reimburse insurers or directly to repair the harm (e.g., fund security improvements after a breach). While insurance is a backstop, it does not reduce our determination to hold the culprit directly accountable via the legal system.

Public Policy and Deterrence: We will publicize this Policy appropriately – key partners and stakeholders (including employees, contractors, and even customers where relevant) will be made aware of it. The Policy may be published in an Employee Handbook, posted on internal portals, and a summary may even be shared on our website or terms of service (especially the notice that we will take legal action against any interference or misuse of our systems). The goal is **deterrence**: would-be "meddlers" should think twice knowing how extensive our response will be. By citing concrete laws and consequences, the Policy puts a sharp edge on our warnings. For example, if we have a partner considering breaching a contract, a reminder that such could constitute tortious interference or fraud with legal liability may dissuade them. Similarly, an IT user considering probing our network without permission might back off knowing it's not just a company policy but a felony (CFAA)[12]. In essence, the Policy is as much a shield as a sword – ideally it prevents incidents from occurring at all.

Continuous Update and Legal Compliance: The Company will review and update this Policy regularly to ensure it remains in line with current laws and emerging threats (for instance, if new cybercrime treaties or laws are passed, or if new forms of interference like AI-driven fraud arise, we will amend the Policy to cover them). This living document approach ensures no gap in coverage. Additionally, we ensure that nothing in this Policy conflicts with any **law or public right**. The Policy is intended to bolster legal protection, not contradict legal obligations. For example, this Policy will not be used to quash legitimate whistleblower activities or employee rights under labor laws – interference as defined here does **not** include lawful reporting of the Company's own wrongdoing or protected concerted activity, and we would not misapply the Policy to such situations. The focus is on unlawful or bad-faith interference. In any enforcement action, the Company will act in good faith and consistent with the rule of law, so that our actions under this Policy will be upheld by courts and authorities.

Documentation and Incident Response: In practice, when an interference incident is detected, the Company will trigger an **Incident Response Plan** that involves legal, security, and management teams. This Policy will guide the legal team's steps in that response. All evidence will be gathered and preserved (to meet standards of proof for court). We will then decide which legal avenues (civil, criminal, or both) to pursue, again referencing the Policy's outlined laws. By having this framework pre-established, our response to incidents will be swift, consistent, and well-coordinated with counsel and law enforcement.

Conclusion: This comprehensive Policy stands as a clear declaration: **VeridicaSystems Corporation will aggressively protect itself using every legal means available when anyone interferes with its business.** Whether the threat comes from a local trespasser, a disgruntled insider, a competitor's unfair tactics, or an international cybercriminal, the Company has a plan – rooted in strong legal authority – to immediately stop the interference and hold the actor accountable. The Policy's reach across **contracts, internal rules, and public law** ensures that it is effective in any scenario where the Company's operations might be "messed with." All persons dealing with VeridicaSystems are hereby on notice that the Company's rights and business continuity are paramount and will be defended vigorously. We consider this Policy not just a company guideline, but a statement of our legal rights and an integral part of our risk management and corporate governance. Through this Policy, VeridicaSystems affirms its unwavering stance: **mess with our business, and you will face consequences – swiftly, certainly, and backed by the full force of the law**.

Sources Cited:

- Pennsylvania tort law on interference with contracts/business: Adler, Barish, Daniels, Levin & Creskoff v. Epstein (Pa. 1978) (recognizing liability for one who "intentionally and improperly interferes" with another's contract)[1]; elements of tortious interference in PA[2].
- Pennsylvania Uniform Trade Secrets Act, 12 Pa. Cons. Stat. § 5302 (definitions of "improper means" including breach of secrecy duty)[6]; § 5303 (injunctive relief for trade secret misappropriation)[18].
- Pennsylvania computer crime statutes: 18 Pa.C.S. § 7611 (Unlawful Use of Computer – unauthorized access)[13]; § 7613 (Computer Theft – using a computer to steal information)[8]; § 7614 (Unlawful Duplication of computer data)[15]; § 7615 (Computer Trespass – e.g. causing malfunction or data alteration)[7]; § 7616 (Distribution of computer virus)[7].
- Definition of criminal trespass in Pennsylvania: 18 Pa.C.S. § 3503(b)(1) (defiant trespasser if one enters or remains in a place where notice against trespass is given)[14].
- Pennsylvania commercial disparagement (business defamation) law: PA Supreme Court in Pro Golf Mfg., Inc. v. Tribune Review (2002) outlining elements of commercial disparagement (false statement, intent or reason to expect financial loss, actual loss, knowledge/recklessness as to falsity)[10]; recognition that businesses have a remedy for false statements harming their products/services[9].
- U.S. Computer Fraud and Abuse Act: DOJ Justice Manual 9-48.000 (explaining CFAA as key law against cybercrimes)[12]; 18 U.S.C. § 1030(a)(5) (illegal to transmit code causing unauthorized damage to a protected computer)[19]; 18 U.S.C. § 1030(a)(7) (illegal to extort via threats to damage a computer or data)[21][22].

- U.S. RICO law: 18 U.S.C. §§ 1961–1962 – RICO allows companies to sue for triple damages and fees when injured by a pattern of racketeering[4][5]; example of using RICO for trade secret theft[4].
- U.S. Hobbs Act: 18 U.S.C. § 1951(a) (crime to obstruct, delay or affect commerce by robbery or **extortion**, including threats of force or fear)[11]; § 1951(b)(2) (defining extortion as obtaining property by wrongful use of actual or threatened force, violence, or fear)[24].
- International IP agreements: WTO's TRIPS Agreement (1995) – binding on all WTO members, setting minimum IP protection standards and requiring equal treatment of foreign IP owners[25][26].
- Council of Europe **Budapest Convention on Cybercrime** (2001): first international treaty on computer crime, obligating parties to criminalize hacking, virus attacks, etc., and to cooperate in investigations[31][32]. (The U.S. is a Party, enabling cross-border pursuit of cybercriminals).

---

[1] [2] Philadelphia Business Lawyers | Tortious Interference

https://www.greatlawyers.com/2017/08/31/tortious-interference-applied-pennsylvania-courts/

[3] [4] [5] [23] "Civil RICO Actions," National Law Journal | News & Resources | Dorsey

https://www.dorsey.com/newsresources/publications/2004/04/civil-rico-actions-national-law-journal

[6] [18] Pennsylvania Uniform Trade Secrets Act | PUTSA | Lawyers | Attorneys

https://hh-law.com/pennsylvania-uniform-trade-secrets-act-putsa/

[7] Unlawful Use of Computer in PA (Maximums and Defenses)

https://www.themcshanefirm.com/pennsylvania-sex-crimes/unlawful-use-of-computer/

[8] [13] [15] [16] What Are the Computer Crimes Statutes in Pennsylvania?

https://www.philadelphiacriminallawyers.com/computer-crimes-statutes-in-pennsylvania/

[9] [10] [17] Commercial Disparagement in Pennsylvania | Wolf, Baldwin & Associates, P.C. | Pottstown Pennsylvania

https://www.wolfbaldwin.com/articles/commercial-litigation-articles/commercial-disparagement-in-pennsylvania/

[11] [24] 18 U.S. Code § 1951 - Interference with commerce by threats or violence | U.S. Code | US Law | LII / Legal Information Institute

https://www.law.cornell.edu/uscode/text/18/1951

[12] Justice Manual | 9-48.000 - Computer Fraud and Abuse Act | United States Department of Justice

https://www.justice.gov/jm/jm-9-48000-computer-fraud

[14] MERRITT v. MANCINI et al, No. 5:2019cv02785 - Document 68 (E.D. Pa. 2022) :: Justia

https://law.justia.com/cases/federal/district-courts/pennsylvania/paedce/5:2019cv02785/558559/68/

[19] [20] [21] [22] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers | U.S. Code | US Law | LII / Legal Information Institute

https://www.law.cornell.edu/uscode/text/18/1030

[25] [26] [27] [28] [29] [30] The Role of International Treaties in Cross-Border IP Enforcement | PatentPC

https://patentpc.com/blog/the-role-of-international-treaties-in-cross-border-ip-enforcement

[31] [32] [33] [34] [35] Text - Treaty Document 108-11 - Council of Europe Convention on Cybercrime | Congress.gov | Library of Congress

https://www.congress.gov/treaty-document/108th-congress/11/document-text