Shut Enterprises LLC
Data Architecture, Privacy, Governance, Risk, and Compliance

[1]

POLICY:
CYBERSECURITY, DATA PRIVACY, AND ARTIFICIAL INTELLIGENCE (AI)

Last Revised: 9/17/2024

[1] Generated by Leonardo.ai on August 12, 2024 at https://app.leonardo.ai/image-generation. See APPENDIX for result choices.

INTRODUCTION

Artificial Intelligence (AI) is a technology in which computer systems ingest large amounts of data to “simulate human intelligence and problem-solving capabilities” (IBM, *What Is AI?*, ¶ 2) by employing “machine learning and deep learning [using] algorithms … modeled after the human brain” (*Id.*, ¶ 2).

AI was first introduced in 1952 and from then until 2012, the “processing power required to train AI on large data sets doubled about every two years” (Brown, 2019, ¶ 12), a concept applied to semiconductor capacity known as Moore’s Law[2] (*Id.*, ¶ 13; Intel, ¶ 1).

Almost 70 years since its invention, AI is still considered to be in its infancy; however, with the advent of powerful cloud computing solutions and the rise of consumer-friendly applications such as Open AI’s ChatGPT in 2023, the technology has boomed, effectively “dwarf[ing] Moore’s Law” (Brown, ¶ 15). AI’s processing power no longer doubles every two years; rather, it does so now in less than 3.4 months (*Id.*, ¶ 14) and is rapidly “transforming our world” in every conceivable way (*Id.*, ¶ 7).

While this new technology offers bold and exciting opportunities for humanity, it also brings untold new risks, threats, and dangers to personal data privacy, ethical business behavior, creative ownership, automated decisioning, and cybersecurity safety that must be defined, developed, implemented, and continuously monitored as the technology evolves over time.

PURPOSE

This Policy will outline Shut Enterprises’ (Shut Ent) stance on cybersecurity, managing and protecting all personally identifiable information on our employees and customers, and outline acceptable usage of enterprise AI for business decisions.

STAKEHOLDERS

Stakeholders include the President/Founder, all firm managers and employees, partners, contractors, and key vendors with whom we carry a contractual relationship to store, process, share, or delete personally identifying information or non-public personal information (PII and/or NPI) (Assignment Instructions, *Research*, bullet 1, sub-bullet 3).

[2] Named for Intel co-founder Gordon Moore from his white paper in 1965. See https://www.intel.com/content/www/us/en/newsroom/resources/moores-law.html#gs.c9t28i for details.

DEFINITIONS

TERM	DEFINITION
AI	Artificial Intelligence, as defined in *Introduction,* ¶ 1
FTC	**Federal Trade Commission**. This U.S. agency is responsible for the establishment and enforcement of all financial institution data privacy regulations related to the Gramm-Leach-Bliley Act of 1999, per 16 C.F.R. § 313.1 *et seq.* See also https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act for detailed information and regulatory guidance.
GDPR	General Data Protection Regulation (May 25, 2018). Regulation that governs all aspects of personal data by customers who are residents of the European Union. Information at https://gdpr.eu/what-is-gdpr/
GLBA	Gramm-Leach-Bliley Act of 1999, passed to regulate data privacy for financial institutions. Regulated by the Federal Trade Commission. 15 U.S.C. § 6801 *et seq* and FTC Regulations at 16 C.F.R. §§ 313.1 *et seq*. Information at https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act
NIST (800-53)	**National Institute of Standards and Technology**, a U.S. governmental agency dedicated to awareness and education on cybersecurity, software vulnerabilities, and technological risk assessments. NIST 800-53 is guidance on how organizations can guard themselves against such risks. Information at https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
PII	**Personally Identifiable Information** refers to any combination of data that can be used to decipher the actual identity of any living person, including one's name, address, phone number, email address, as well as biometric information, religion, nationality, race, etc. Full details on PII may be found within the FTC's GLBA regulation guidance at https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act
VPN	**Virtual Private Network** refers to a network provider who encrypts digital traffic using a corporate security system designed to "keep[] … online activity hidden and protect[] your privacy." See Norton Privacy Blog at https://us.norton.com/blog/privacy/what-is-a-vpn

POLICY

Cybersecurity

1. As Shut Ent may store and process sensitive nonpublic personal consumer and customer information (NPI), at a minimum, it shall comply with standing FTC regulations in the **GLBA Safeguards Rule** (16 C.F.R. §§ 314.1 – 314.6), including the creation and maintenance of a detailed Incident Response Plan, periodically updated to cover corporate risk appetites and severity levels, mitigation of newly-identified and residual risks, compensating controls, and consequence models. 16 C.F.R. § 314.3 *et seq*.

2. There shall be specific **written procedures** to ward against **cybersecurity** attacks, such as Denial of Service (NIST, *Denial of Service Protection*, p. 296), "Threat Hunting" (NIST, *Threat Hunting*, RA-10, pp. 247-248), signs of intrusion (NIST, *Indicators of Compromise,* p. 343), vulnerability scanning and remediation (NIST*, Vulnerability Monitoring and Scanning,* RA-5, pp. 242-245), and other best practices to protect the safety, integrity, and soundness of the firm's digital environments. See also 15 U.S.C. § 6801(b)(2); 16 C.F.R. § 314.3(b)(2).

3. All corporate digital activity shall take place from within the firm's virtual private network (**VPN**), in alignment with not only the above-stated GLBA regulations, but also the U.S. National Institute of Standards and Technology's (**NIST**) most recent guidelines entitled the "Security and Privacy Controls for Information Systems and Organizations", also known as the **NIST 800-53** (NIST, *Remote Access - Discussion*, p. 48).

4. Corporate file systems and databases must leverage **user role-based controls** to ensure that only persons with a bona-fide business purpose can access them (NIST*, Access Enforcement – Restrict Access to Specific Information* Types, *Discussion*, p. 27). See also 16 C.F.R. § 314.4(c)(1)(i, ii).

5. Deploy trusted, secure, and consistent mechanisms to assess if corporate networks have either been infiltrated or their data tainted (NIST*, Tainting,* SI-20, pp. 360-361). 16 C.F.R. § 314.4(c)(8).

Data Privacy

1. **Shut Enterprises shall <u>not</u> share, sell, lend, enable access to, or show any authentic prospect or customer personal data without prior and verified written client consent.**

2. Whenever Shut Ent advises Financial Institutions, it shall be subject to regulations under the Gramm-Leach-Bliley Act of 1999 (**GLBA**); therefore, the company shall abide by all of its statutory (15 U.S.C. § 6801 *et seq.*) and related regulatory (16 C.F.R. § 313.1 *et seq.*) requirements; *as follows*:

    a. The firm shall implement an effective and comprehensive **data governance program** to inventory nonpublic personal data (NPI) and to document, protect, and preserve all Production data quality, in accordance with the requirements of the GLBA *Privacy Rule* (De Groot, *Privacy Rule*, ¶ 6) and NIST 800. NIST, *Personally Identifiable Information Quality Management*, PM-22, pp. 215-216; NIST, *Data Governance Body*, PM-23, p. 216; NIST, *Data Integrity Board*, PM-24, p. 216.

    b. Annual GLBA employee **training** and **compliance exams** must be successfully completed by all staff to monitor the firm's adherence to this critical banking and data privacy law. 16 C.F.R. § 314.4(e).

    c. Finally, based on GLBA FTC regulations and the additional guidance from the NIST 800-53, sensitive data on any digital platform shall always be strongly **encrypted**, either in-transit or at-rest. If data cannot be encrypted, the firm must institute adequate compensating controls to ensure security. 16 C.F.R. § 314.4(c)(3); NIST, *Discussion*, p.27; *Protection of Information At Rest*, SC-28 and related controls, pp. 316-317.

3. All other industries shall be subject to provisions defined in appropriate U.S. Federal and State regulations, such as in this emergent listing:

Federal:

a. General Privacy:
Privacy Act of 1974
5 U.S.C. § 552a

b. Cyber / Technology:
Computer Fraud and Abuse Act (CFAA, 1984)
18 U.S.C. § 1030

c. Healthcare/Insurance/Government:
Healthcare Insurance Portability and Accountability Act
P.L. 104-191; Five Rule Summaries: HIPAA, 1996

d. Financial Institutions:
Gramm-Leach-Bliley Act of 1999
15 U.S.C. §§ 6801-6809; Rules: GLBA (Privacy) and Safeguards, 1999

e. Children:
Children's Online Privacy Protection Act
15 U.S.C. §§ 6501-6508; Rule: COPPA, 1998

f. Education:
Family Educational Rights and Privacy Act
20 U.S.C. § 1232g, Rule: FERPA, 2000

g. Other Acts as catalogued by the Congressional Research Service (CRS)

State:

a. California Consumer (Rights) Privacy Act (CCPA / CPRA, 2018; amended 2023)

b. Colorado Privacy Act (CPA, 2023)

International

a. Australia GDPR (Australian Privacy Act, 1988)

b. General Data Protection Regulation (GDPR, European Union, 2018)

c. Brazil LGPD (2018)

d. UK GDPR (2018; Brexit 2022)

e. EU AI Act (2021; amended 2024)

AI Prompting and Results

1. Once data is secured, the firm shall "minimize" the presence of nonpublic personal information (NPI) and personally identifiable information (PII) in file systems or databases as designed for

    a. 1) "**internal testing, training,** and **research**" in general (NIST, *Minimization of Personally Identifiable Information Used in Testing, Training, and Research*, PM-25*,* p. 217)

    and

    b. any platforms sourced by **Artificial Intelligence (AI)**.

2. The firm shall use the emerging EU AI Act (EP, 2024) as guidance to classify the Risk Level of user prompting of all corporate AI platforms, as follows:

    a. **"Unacceptable Risk"** (EP, *Unacceptable Risk*)

        i. Employees and contractors must **never** **--** ***not in test nor in jest*** **--** engage in prompts that deliver this level of risk to the enterprise or result in the following scenarios:

            1. "**Cognitive Behavioral Manipulation**" (*Id*., bullet 1), including but not limited to "voice-activated toys that encourage dangerous behavior in children" (*Id.*), step-by-step instructions on how to build a bomb, advice on how to commit terrorist acts, and/or detailed steps on how best to launder money.

            2. "**Social Scoring**" (*Id.*, bullet 2), which seeks to rank people on "behavior, socio-economic status or personal characteristics" (*Id.*)

                a. Allowing AI prompts under these circumstances would also trigger violations of U.S. laws, namely Title VII of the Civil Rights Act of 1964 and the Age Discrimination Act of 1975, biases that already existed in society prior to AI and shall not be exacerbated by it.

            3. "**Biometric** identification and categorization of people" (*Id*., bullet 3)

                a. Allowing AI prompts under these circumstances would also trigger violations of U.S. laws, namely the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Americans with Disabilities Act of 1992 (ADA).

4. “**Real-time and remote biometri**c identification systems, such as facial recognition” (*Id.,* bullet 4)

    a. *Allowing AI prompts under these circumstances may trigger the U.S. laws stated above, as the AI may introduce unwanted and illegal bias and judgments against nationality, skin color, race, age, etc.*

ii. Finally, employees shall **refrain** from using corporate AI platforms to prompt results of a sexual/pornographic nature, seek guidance on how to perform human trafficking and child exploitation, where and how to obtain illegal drugs and alcohol, how to commit illegal commerce (such as smuggling, money laundering, bribery, pay-to-play), or any other actions or behaviors that would be deemed as violent, dangerous, deviant, or socially crude actions to a reasonable person.

1. **Note**: Even if the AI platform itself is programmed to prohibit responses to such prompts, these prompt categories violate WW’s Code of Conduct and Ethics, may be illegal, and will be subject to the terms of the Policy Violation Consequence Model on the final page.

b. **“High Risk”** (EP*, High Risk*, ¶ 1) and 2))

i. Per the EU AI Act, and used as policy guidance here, High Risk AI systems are those that deal in “management and operation of critical infrastructure … education and vocational training … employment, worker management and access to self-employment … essential [public] and private services and benefits … law enforcement … migration, asylum and border control … [and] assistance in legal interpretation and application of the law.”

1. *At Shut Ent, this provision would immediately apply to data obtained from HR and/or Law platforms, such as ADP, SAP HRIS, NetSuite, Westlaw, LexisNexis, etc., but additional platform approvals and restrictions shall be considered on a business purpose, case-by-case basis.*

c. **“Transparency Requirements”** (*Id.*, *Transparency Requirements*)

i. Whenever employees produce any AI-generated images, audio, video, writings, chats, booklets, pamphlets, or any other content for official corporate marketing, account management, lending, advising, and/or any final decisioning, it must be followed by a clear and conspicuous label or citation that the content was **AI-Generated** (EP, ¶ 3).

ii. Before generating content that is a known restricted name or trademark, employees should verify usage with Enterprise Risk and Compliance (ERC) and/or General Counsel (NLR, *Intellectual Property Risks*, ¶ 1). Examples include the Nike “swoosh” and the iconic white apple for “Apple Computing.”

TRAINING, MONITORING, AND REPORTING

Training

1. Shut Enterprises shall create an **AI Best Practices Guidebook** as a basis for employee referential support and ongoing training. (NLR, *Addressing The Risks*, ¶ 1).

   a. For departments where AI could be most effective, WW’s Enterprise Risk and Compliance Department will partner with Human Resources to offer periodic training on ethical and effective AI usage in the workplace.

   b. Employees will be assessed at least once yearly on these skills as part of an ongoing Compliance Training program.

      i. The exam shall evaluate the employee’s understanding of AI use in the following areas:

         > “Confidentiality … Personal Data and Privacy Violations … Quality Control … [Customer, Job Candidate, and Employee] Bias and Discrimination … Product Liability ... Intellectual Property Ownership … Misrepresentation … Insurance Coverage [and] Future Requirements” (NLR*, Understanding the Risks,* ¶¶ 1-12).

   c. If an employee fails the exam after three successive attempts, the employee’s department manager shall be notified and must open an IT support ticket to revoke all employee AI access until such time that the employee is able to pass the exam.

   d. Remedial training may be ordered to close gaps in understanding and assist in exam passage.

   e. Enterprise Compliance and Risk shall also follow this Policy with specific *procedures* covering which employees may be granted access to AI platforms and all controls exercised with that privilege and responsibility. (NLR, *Addressing The Risks,* ¶ 1).

Monitoring and Reporting

On a regular basis, Shut Enterprises' Information Technology department shall produce a report with an anonymous summary by department of the kinds of prompts and commands that employees are requesting of the AI.

1. Should any **Unacceptable Risk Prompts** be discovered (see pp. 5-6 of this Policy), Enterprise Risk and Compliance shall immediately open an investigation and notify the Department manager of the nature of the prompt(s). See the "Policy Violation Consequence Model" on page 9.

2. In addition to monitoring Unacceptable Risk prompts, Enterprise Risk and Compliance shall also establish structured Quality Control procedures that require select managers and data governance stewards to review AI results in the following risk areas:

    i. "Factual Inaccuracies" (NLR, *Addressing The Risks*, ¶ 5)

    ii. "Confidentiality and Privacy" (*Id.*, ¶ 2)

    iii. "Intellectual Property" (*Id*., ¶ 6)

    iv. Enterprise "Misrepresentation" Issues (*Id*., ¶ 7)

    v. "Insurance" (*Id*., ¶ 8)

    vi. "Regulations" (*Id.,* ¶ 9)

    vii. "Employment" Evaluation and Decisioning (*Id*., ¶ 10)

3. Each Department Head must perform weekly Quality Control to review incomplete or inaccurate results and assume accountability for correcting any underlying AI Training Data entries that may have caused them (NLR, *Addressing The Risks*, ¶ 1).

4. There shall also be an executive summary-level (Dashboard) and department-level (Detailed) report distributed to appropriate levels of management regarding the accuracy of enterprise-wide AI usage (NLR, *Addressing The Risks*, ¶¶ 1-11) and recommendations for ongoing improvement.

5. Finally, Enterprise Risk and Compliance shall summarize and report these results at least annually, but preferably quarterly, to Senior Management and the firm's Board of Directors.

Policy Violation Consequence Model

In closing, AI usage at Shut Enterprises is an uncharted privilege, with inherent risks to our company and customers' lives that must be managed with care.

To this end, Shut Enterprises operates under a Zero-Tolerance Consequence Model regarding Unacceptable Risk Prompts.

- Should an Unacceptable Risk AI prompt or result be discovered in weekly Production AI reporting, an internal investigation will be opened by Enterprise Risk and Compliance (ERC).
- If an employee is purposely and actively engaging in such prompting, ERC will contact the employee's manager(s) and Human Resources with details of the investigation and next steps.
- Consequences for violating the Unacceptable Risk portion of the Policy may include immediate revocation of employee AI privileges, termination of employment, law enforcement involvement, legal prosecution, or all of the above.

High Risk Violations may include the actions listed above; however, depending on the nature, categorization, and frequency of the questionable prompts, lesser consequences may also include employee remedial training, unfavorable annual reviews, and/or introduction of a performance improvement plan (PIP).

REFERENCES

- 15 U.S.C. §§ 6801- 6827; Pub. L. 106-102, Title V, § 501; 113 Stat. 1436 (Nov 12, 1999), *Gramm-Leach-Bliley Act of 1999*, Office of the Law Revision Counsel, United States Code. Sourced on Jul 23, 2024 from https://uscode.house.gov/view.xhtml?req=(title:15%20section:6801%20edition:prelim) and cited by statutory code and section.

- 16 C.F.R. §§ 314.1 – 314.6; 67 FR 36493 (May 23, 2002), *Gramm-Leach-Bliley Act of 1999.* Code of Federal Regulations, National Archives and Records Administration. Sourced on Jul 23, 2024 from https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314 and cited by regulatory code and part.

- Natasha Allen, Chanley T. Howell, et al. of Foley & Lardner LLP, *My Employees Are Using ChatGPT. What Now?*, Jul 17, 2023, The National Law Review. Sourced on Jul 29, 2024 from https://natlawreview.com/article/my-employees-are-using-chatgpt-what-now and cited as (NLR).

- Jeff Brown, *How Fast Is AI Advancing? Take a Look at This Chart …,* Nov 19, 2019, The Bleeding Edge (Blog), Brownstone Research. Sourced on Jul 28, 2024 from https://www.brownstoneresearch.com/bleeding-edge/how-fast-is-ai-advancing-take-a-look-at-this-chart/ and cited as (Brown).

- De Groot, Juliana (May 6, 2023), *What is GLBA Compliance? (Understand Requirements)*. Digital Guardian – Data Insider Blog. Sourced on Jul 23, 2024 from https://www.digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act and cited as (De Groot)

- European Parliament, *EU AI Act: first regulation on artificial intelligence*, Aug 6, 2023; last revised Jun 18, 2024. Sourced on Jul 27, 2024 from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence and cited as (EP).

- IBM Editors, *What Is artificial intelligence (AI)?,* (Undated), IBM. Sourced on Jul 28, 2024 from https://www.ibm.com/topics/artificial-intelligence and cited as (IBM).

- Intel Newsroom, *Moore's Law*, Intel, Sep 18, 2023. Sourced on Jul 27, 2024 from https://www.intel.com/content/www/us/en/newsroom/resources/moores-law.html#gs.c9t28i and cited as (Intel).

- *NIST SP 800-53 Rev* 5, Sep 2020, revised in patch on Nov 7, 2023, National Institute of Standards and Technology. Sourced on Jul 28, 2024 from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final and cited as (NIST).

CONTACTS

NAME	TITLE	EMAIL
Kathryn L. Shut	President, Founder	info@shutentllc.com

VERSION LOG

VERSION	EDITOR	COMMENTS
1.0	Kathryn L. Shut	Initial Document