

Security Code of Conduct

2.1. Introduction

Purpose: This Security Code of Conduct ("Code") establishes the expected standards of behavior for all World Bank personnel concerning the security of the Bank's information, systems, physical premises, and other assets. Adherence to this Code is fundamental to fostering and maintaining a strong, pervasive security culture throughout the organization.

Commitment to Security: World Bank is unequivocally committed to the highest standards of security to protect customer data, proprietary business information, intellectual property, and the overall integrity of our operations. We recognize that maintaining the trust placed in us by our customers, shareholders, and regulatory bodies is paramount. Every individual associated with World Bank shares a collective and personal responsibility for upholding these security standards in all their professional activities. The ethos of JPMorganChase, emphasizing operation with the highest level of integrity and ethical conduct, serves as a guiding principle for World Bank's approach.

Applicability: This Security Code of Conduct applies to all individuals working for or on behalf of World Bank, irrespective of their employment status or location. This includes all full-time and part-time employees, members of the Board of Directors, corporate officers, contractors, consultants, temporary staff, and any other third parties granted access to Bank assets or information.

Guiding Principle: The core principle underpinning this Code is to always "Do the right thing - not necessarily the easy or expedient thing". This means prioritizing security and ethical considerations in all decisions and actions, even when faced with pressures or perceived inconveniences.

2.2. Protecting Confidential Information

2.2.1. Definition of Confidential Information: Confidential Information encompasses a broad range of data and knowledge that is critical to World Bank's operations and reputation. This includes, but is not limited to: * Customer Personally Identifiable Information (PII) such as names, addresses, account numbers, Social Security numbers, dates of birth, and contact details. * Customer financial records, transaction histories, credit card numbers, loan details, and investment information. * World Bank's strategic plans, financial results (before public release), product development details, internal operational procedures, and security configurations. * Intellectual property, including proprietary software, algorithms, trademarks, and copyrighted materials. * Employee data, such as personnel records, salary information, and performance reviews. * Any information designated as "Confidential," "Restricted," or "Internal Use Only" under the Bank's Data Classification Policy. * Any other non-public information that, if disclosed, could harm World Bank, its customers, or its employees.

Rationale: A clear definition is essential for employees to understand the scope of information requiring protection.

2.2.2. Handling Confidential Information: Confidential Information must be accessed, used, processed, stored, and shared strictly on a "need-to-know" basis. This means access is limited only to those individuals whose job responsibilities explicitly require it for legitimate World Bank business purposes. Curiosity or convenience are not acceptable reasons for accessing confidential data. *Rationale:* Limits exposure of sensitive data, reducing the risk of unauthorized disclosure or misuse.

2.2.3. Non-Disclosure: Personnel must not discuss or disclose Confidential Information in public places, including elevators, cafeterias, public transport, or even within World Bank common areas if conversations can be overheard by unauthorized individuals. Extreme caution must be exercised when discussing sensitive matters over speakerphones or mobile phones in public. Confidential Information must never be disclosed on personal social media accounts, blogs, forums, or to unauthorized individuals, including family and friends. *Rationale:* Prevents inadvertent disclosure of sensitive information through casual conversations or insecure communication channels.

2.2.4. Securing Physical Documents: Physical documents (printouts, notes, reports) containing Confidential Information must be stored securely when not in active use. This includes using locked drawers, filing cabinets, or secure office spaces. Documents should not be left unattended on desks, in meeting rooms, or in other accessible areas. *Rationale:* Addresses the risk of physical data breaches through lost or stolen documents.

2.2.5. Secure Transmission: When transmitting Confidential Information electronically, whether internally or externally, only Bank-approved secure methods must be used. This typically includes encrypted email services, secure file transfer protocols (SFTP), or other Bank-sanctioned encrypted communication channels. Sending Confidential Information via unencrypted email or personal messaging apps is strictly prohibited. *Rationale:* Protects data in transit from interception or unauthorized access.

2.3. Acceptable Use of Bank Systems and Assets

2.3.1. Business Use Priority: World Bank's Information Technology (IT) systems, including computers, networks, internet access, email systems, software applications, and telecommunication devices, are provided primarily for conducting official Bank business. Limited and incidental personal use may be permitted provided it: * Does not interfere with the employee's work performance or the work of others. * Does not consume excessive Bank resources (e.g., bandwidth, storage). * Does not violate any other provision of this Code or other Bank policies. * Occurs during non-work time (e.g., breaks, outside of scheduled work hours). *Rationale:* Clarifies the primary purpose of Bank IT assets while allowing for reasonable personal use under strict conditions.

2.3.2. Prohibited Activities: Users must not use World Bank systems or assets for any of the following activities: * Any illegal or fraudulent activities, including but not limited to unauthorized financial transactions, money laundering, or identity theft. * Harassment, discrimination, or creating a hostile work environment. * Accessing, storing, displaying, or distributing pornographic, obscene, defamatory, or otherwise offensive or inappropriate material. * Unauthorized commercial activities, personal business ventures, or soliciting for personal gain. * Political campaigning or lobbying, unless explicitly authorized as part of official Bank duties. * Knowingly introducing malware, viruses, or other malicious software. * Attempting to circumvent security controls or gain unauthorized access to systems or data. * Any activity that could damage the Bank's reputation, compromise its security, or lead to legal liability. *Rationale:* Sets clear boundaries for unacceptable behavior, protecting the Bank from legal, reputational, and security risks.

2.3.3. Respect for Intellectual Property: Personnel must respect all intellectual property rights, including copyrights and trademarks. Do not illegally copy, download, install, or distribute copyrighted software, music, videos, documents, or other materials using Bank systems. All software used on Bank equipment must be properly licensed and approved by the IT department. *Rationale:* Ensures compliance with intellectual property laws and prevents legal liabilities for the Bank.

2.3.4. No Expectation of Privacy: Users should have no expectation of privacy regarding any information created, stored, sent, or received using World Bank's IT systems and networks. World Bank reserves the right to monitor, access, review, and disclose any and all system usage, including email messages, internet activity, file access, and application usage, without prior notice to the user. This monitoring may be conducted for purposes including, but not limited to, ensuring compliance with Bank policies, investigating security incidents, meeting legal and regulatory obligations, and maintaining system performance. *Rationale:* Informs users that their activities on Bank systems are subject to monitoring, which is necessary for security and compliance.

The scope of a Security Code of Conduct has significantly broadened from traditional Acceptable Use Policies. It now deeply integrates crucial aspects such as data privacy, the specific security demands of remote work, and overarching ethical considerations. This evolution reflects a more holistic understanding of an employee's role and responsibility in the modern cybersecurity landscape. For World Bank, this necessitates a comprehensive Code that is not static but is regularly reviewed and updated to address new work modalities, emerging threat vectors, and evolving regulatory expectations. This Code serves as a central document for shaping the overall security culture and mitigating diverse risks that can stem from employee actions or negligence across various operational contexts.

2.4. Password Security and Management

2.4.1. Individual Responsibility: Each user is personally responsible for the security of all passwords and authentication credentials associated with their World Bank accounts. This

responsibility cannot be delegated. *Rationale:* Reinforces personal accountability for a critical security control.

2.4.2. Strong Passwords: Users must create strong, unique passwords for all World Bank systems and applications they access. Passwords must comply with the Bank's Password Policy, which typically requires: * A minimum length of 12 characters. * A combination of uppercase letters, lowercase letters, numbers, and special symbols (e.g., !@#%^&*). * Avoidance of dictionary words, common phrases, personal information (names, dates), or sequential characters (e.g., "12345", "abcde"). *Rationale:* Complex passwords are significantly more resistant to guessing, brute-force attacks, and dictionary attacks.

2.4.3. Confidentiality of Passwords: Passwords must never be shared with anyone, including colleagues, managers, IT support staff, family, or friends. IT personnel will never ask for a user's password. Users must not write passwords down in unsecured locations (e.g., sticky notes, notebooks left on desks) or store them in unencrypted files on computers or mobile devices. The use of Bank-approved password managers is encouraged for managing multiple complex passwords. *Rationale:* Prevents unauthorized access through shared or improperly stored credentials.

2.4.4. Regular Password Changes: Users are required to change their passwords at regular intervals as mandated by the Bank's Password Policy (e.g., every 90 days for standard user accounts, every 60 days for privileged accounts). Passwords must also be changed immediately if there is any suspicion that they may have been compromised. *Rationale:* Limits the duration for which a compromised password can be used.

2.4.5. Use of MFA: Users must comply with all Multi-Factor Authentication (MFA) requirements when accessing Bank systems that mandate its use (e.g., remote access, sensitive applications). Users must protect their MFA tokens (hardware or software) with the same diligence as their passwords. *Rationale:* MFA is a critical layer of security; user compliance is essential for its effectiveness.

2.5. Data Handling and Classification

2.5.1. Adherence to Data Classification: All personnel must understand and adhere to World Bank's Data Classification Policy. This policy categorizes data into levels such as Public, Internal Use Only, Confidential, and Restricted, based on its sensitivity and impact if compromised. Data must be handled, stored, transmitted, and disposed of according to the specific requirements of its classification level. *Rationale:* Ensures that data is protected according to its sensitivity and value to the Bank.

2.5.2. Secure Storage: Electronic data, particularly Confidential or Restricted information, must be stored on Bank-approved and secured network drives, encrypted devices, or approved cloud storage solutions. Storing sensitive Bank data on personal, unsecured devices (e.g., personal USB drives, personal cloud accounts like Dropbox or Google Drive) is strictly prohibited unless explicitly authorized under a BYOD policy and with appropriate

security controls in place. *Rationale:* Prevents data loss or unauthorized access due to storage on insecure or unmanaged media.

2.5.3. Secure Disposal: Physical documents containing sensitive or Confidential Information must be disposed of using Bank-approved shredders or placed in designated confidential waste bins for secure destruction. Electronic media (e.g., hard drives, USB drives, CDs/DVDs) containing such information must be securely wiped or physically destroyed according to Bank standards before disposal or repurposing. *Rationale:* Prevents data recovery from improperly disposed media, which could lead to data breaches.

2.6. Clean Desk and Clear Screen Policy

2.6.1. Clean Desk: Personnel are required to maintain a "clean desk" environment. This means that when workstations are unattended, and always at the end of the workday, desks and surrounding work areas must be cleared of all sensitive or Confidential Information in physical form. This includes papers, printouts, notebooks, removable media (USB drives, CDs), and portable electronic devices. Such items must be securely stored in locked drawers, cabinets, or other approved secure containers. *Rationale:* Reduces the risk of unauthorized individuals viewing or stealing sensitive information left unattended. This is a simple yet effective measure to protect physical data.

2.6.2. Clear Screen: Computer screens must be "cleared" by locking the workstation (e.g., using Ctrl+Alt+Del and selecting "Lock," or Windows Key + L) whenever an employee leaves their workstation unattended, even for brief periods such as going to a meeting or taking a short break. Automatic screen locking will also be enforced by IT systems after a short period of inactivity (e.g., 5-10 minutes). *Rationale:* Prevents unauthorized viewing of information on an unattended screen and unauthorized use of an unlocked workstation.

2.6.3. Printers and Copiers: Printed documents, especially those containing sensitive or Confidential Information, should be collected promptly from printers, copiers, and fax machines. Users should verify they have collected all pages of their print job. Any unneeded copies or misprints containing sensitive information must be immediately disposed of in designated confidential waste bins or shredded. *Rationale:* Prevents sensitive documents from being left on shared devices where they could be picked up by unauthorized individuals.

The "Clean Desk and Clear Screen Policy" is not merely about maintaining a tidy workspace; it is a critical physical security measure that directly supports and reinforces logical security controls. Logical access controls, such as passwords and MFA, are designed to protect systems when users are actively interacting with them. However, if a user leaves their workstation unlocked with sensitive data displayed on the screen (a violation of the clear screen principle), or leaves printed confidential documents openly on their desk (a violation of the clean desk principle), an unauthorized individual could potentially bypass these logical controls by simply viewing the screen or taking the physical documents. This demonstrates a direct and crucial link: robust physical security practices, like those mandated by the clean desk and clear screen policy, are essential for maintaining the integrity and effectiveness of

logical security measures. One cannot be fully effective without the diligent application of the other.

2.7. Physical Security Responsibilities

2.7.1. Access Badges: All personnel must wear their official World Bank employee identification badges visibly at all times while on Bank premises. Access badges are non-transferable and must not be shared or lent to anyone, including other employees. Lost or stolen badges must be reported immediately to the Physical Security department or the IT Help Desk. *Rationale:* Enables easy identification of authorized personnel and helps control access to Bank facilities.

2.7.2. Visitor Escort: Visitors must be escorted by an authorized World Bank employee at all times while in non-public areas of the Bank. Personnel are responsible for their visitors and must ensure they do not access unauthorized areas or information. Any unescorted or unidentified individuals observed in non-public areas should be politely challenged or reported to Physical Security. *Rationale:* Prevents unauthorized individuals from freely roaming Bank premises and potentially accessing sensitive areas or information.

2.7.3. Secure Areas: Access to designated secure areas, such as data centers, server rooms, cash vaults, and record storage rooms, is strictly controlled and limited to authorized personnel only. Personnel must not attempt to enter secure areas for which they do not have explicit authorization, nor should they allow or facilitate unauthorized individuals to enter these areas. Secure doors should not be propped open. *Rationale:* Protects critical infrastructure and highly sensitive assets from unauthorized physical access.

2.7.4. Tailgating Prevention: Personnel must actively prevent "tailgating" or "piggybacking," which occurs when an unauthorized person follows an authorized individual through a secure access point (e.g., a door controlled by a badge reader). Each individual entering a secure area must use their own access badge. Be aware of who is behind you when entering secure areas. *Rationale:* Tailgating is a common method used to bypass physical access controls.

2.8. Social Media Use

2.8.1. Professional Conduct: When identifying oneself as a World Bank employee on any social media platform (including personal accounts, professional networking sites like LinkedIn, or public forums), personnel must maintain a high standard of professionalism. It is strictly prohibited to disclose any Confidential Information related to World Bank, its customers, its operations, or its employees. This includes posting internal documents, discussing customer transactions, or revealing non-public strategic information. *Rationale:* Protects the Bank's reputation and prevents the leakage of sensitive information through informal channels. Guidelines from institutions like the British Business Bank and Community Savings Bank emphasize this.

2.8.2. No Endorsement: Personal opinions or statements made by employees on social media should not be presented in a way that could be reasonably construed as an official

statement or endorsement by World Bank, unless explicitly authorized by the Bank's official communications department (e.g., Marketing or Corporate Communications). A disclaimer may be appropriate if there is potential for ambiguity. *Rationale:* Avoids misrepresentation of the Bank's official stance or policies.

2.8.3. Reporting Concerns: Personnel should promptly report to their manager, HR, or the Legal department any social media activity they encounter (whether by employees or external parties) that could potentially harm World Bank's reputation, compromise its security, disclose confidential information, or violate this Code. *Rationale:* Enables the Bank to address potentially damaging social media content quickly.

2.8.4. Use of Bank Social Media: Only personnel specifically authorized by the Marketing or Corporate Communications department may post content on official World Bank social media accounts (e.g., the Bank's official Facebook page, Twitter handle, LinkedIn company page). All official posts must adhere to Bank communication guidelines and be approved through the designated channels. *Rationale:* Ensures consistency, accuracy, and brand alignment in official Bank communications.

2.9. Remote Work Security Guidelines

2.9.1. Secure Environment: When working remotely (e.g., from home or another approved location), personnel must ensure their physical work environment is secure. This includes taking measures to prevent unauthorized individuals (including family members or visitors) from viewing sensitive Bank information on screens or documents, or from accessing Bank-owned equipment. *Rationale:* Extends physical security principles to remote work locations.

2.9.2. Secure Network Connection: Remote work must be conducted using a secure internet connection. If using a home Wi-Fi network, it must be protected with strong WPA2 or WPA3 encryption and a complex, unique password. All access to World Bank's internal network and systems from remote locations must be established through the Bank-approved Virtual Private Network (VPN). The use of unsecured public Wi-Fi (e.g., in cafes, airports) for accessing sensitive Bank systems or data is strongly discouraged and may be prohibited for certain types of work. *Rationale:* Protects data in transit and ensures remote connections are made through a secure, encrypted channel.

2.9.3. Bank-Owned Equipment: Whenever possible, personnel should use Bank-issued and managed equipment (laptops, mobile phones) for remote work. If a Bring Your Own Device (BYOD) arrangement is permitted by specific Bank policy for certain roles or tasks, the personal device must be registered with IT and must meet all Bank-mandated security standards, including endpoint protection software, encryption, and up-to-date patching. *Rationale:* Bank-owned equipment is configured and managed to meet security standards. BYOD introduces risks that must be carefully managed.

2.9.4. Data Protection: All rules and procedures for handling Confidential Information and adhering to data classification standards apply equally to remote work environments.

Sensitive Bank data should not be downloaded or stored on personal devices or personal cloud storage services unless explicitly authorized and protected by Bank-approved encryption and security measures. *Rationale:* Ensures consistent protection of Bank data regardless of work location.

2.9.5. Confidential Conversations: When conducting confidential conversations (e.g., phone calls, video conferences) involving sensitive Bank or customer information while working remotely, personnel must take precautions to ensure these conversations cannot be overheard by unauthorized individuals. This may involve using a private room or headphones. *Rationale:* Prevents eavesdropping and inadvertent disclosure of confidential information in remote settings.

2.10. Reporting Security Incidents and Weaknesses

2.10.1. Obligation to Report: All personnel have a critical responsibility to promptly report any suspected or actual security incidents, observed vulnerabilities in systems or processes, or violations of this Security Code of Conduct or other security policies. Reports should be made to the employee's direct manager, the IT Help Desk, or directly to the Security Operations Center (SOC) through established channels. There will be no retribution for good-faith reporting. *Rationale:* Early reporting is crucial for timely incident response and mitigation of potential damage. Procedures for reporting breaches and security incidents emphasize promptness.

2.10.2. Examples of Reportable Incidents: Incidents that must be reported include, but are not limited to: * Loss or theft of Bank-owned devices (laptops, mobile phones, USB drives). * Suspected or confirmed malware or virus infections. * Receiving or clicking on a suspected phishing email or malicious link. * Any unauthorized access to Bank systems, data, or physical premises. * Suspected or actual data breaches (disclosure of Confidential Information to unauthorized parties). * Discovery of a system vulnerability. * Unexplained system behavior or anomalies. *Rationale:* Provides clarity on what constitutes a reportable incident.

2.10.3. Cooperation with Investigations: All personnel must cooperate fully and truthfully with any investigations into security incidents or policy violations conducted by IT Cybersecurity, Internal Audit, HR, or other authorized Bank departments. *Rationale:* Facilitates effective investigation and resolution of security issues.

A well-communicated and consistently enforced Security Code of Conduct is a primary mechanism for reducing human error, which remains a leading contributor to security breaches. The effectiveness of this Code is significantly amplified when it is deeply integrated with comprehensive security awareness training programs and supported by clear, accessible incident reporting procedures. The Code establishes the explicit expectations for secure behavior (e.g., password security, data handling, clean desk practices). Security awareness training reinforces the "why" behind these rules and teaches the "how" to comply and recognize threats. Clear incident reporting channels empower employees to act as an early

warning system when they observe or suspect something amiss. This synergy—clear rules from the Code, understanding fostered by training, and the means to report issues—collectively strengthens the Bank's human firewall.

2.11. Prohibition of Unauthorized Software/Hardware

2.11.1. Software Installation: Personnel must not download, install, or use any unauthorized software on Bank-owned computers or other devices. All software required for business purposes must be approved by the IT department, be properly licensed, and typically will be installed by authorized IT personnel or through approved software deployment mechanisms. The use of pirated, unlicensed, or unverified software is strictly prohibited. *Rationale:* Prevents the introduction of malware, vulnerable software, or licensing issues into the Bank's environment.

2.11.2. Hardware Connection: Personnel must not connect unauthorized hardware to World Bank's network or to Bank-owned devices without explicit prior approval from the IT department. This includes personal USB drives, external hard drives, personal mobile phones used for tethering, wireless access points, or any other peripheral that has not been vetted and approved by IT. *Rationale:* Unauthorized hardware can introduce security vulnerabilities, malware, or create unmonitored network access points.

2.11.3. Use of Personal Devices (BYOD): If World Bank has a formal Bring Your Own Device (BYOD) policy that permits the use of personal devices for certain work-related tasks, such use is strictly governed by that policy. Personal devices used under a BYOD agreement must be registered with IT, meet all Bank-mandated security requirements (e.g., endpoint security software, encryption, strong passcodes, remote wipe capability), and users must consent to Bank oversight of security configurations on the device as it pertains to Bank data. *Rationale:* Ensures that personal devices accessing Bank resources meet minimum security standards to protect Bank data.

2.12. Ethical Conduct and Avoiding Conflicts of Interest

2.12.1. Integrity and Honesty: All personnel are expected to conduct World Bank business and perform their duties with the highest level of personal and professional integrity, honesty, and ethical standards. *Rationale:* Forms the bedrock of trust within the organization and with customers and regulators.

2.12.2. Prohibition of Misuse of Assets: Bank property, information (including Confidential Information), systems, or an individual's position within the Bank must not be used for personal gain, to benefit friends or relatives, or to engage in activities that compete with World Bank's legitimate business interests. This includes insider trading based on non-public information. *Rationale:* Prevents fraud, abuse of position, and conflicts of interest.

2.12.3. Reporting Unethical Behavior: Personnel have a responsibility to report any suspected unethical behavior, illegal activities, fraud, or significant conflicts of interest they become aware of. Reports can be made to a manager, Human Resources, the Compliance

department, the Legal department, or through the Bank's confidential whistleblower hotline, if available. Reports made in good faith will be protected from retaliation. *Rationale:* Encourages a culture of accountability and provides safe channels for raising serious concerns.

2.13. Compliance with Laws and Regulations

2.13.1. Adherence to Legal Requirements: All personnel must comply with all applicable local, national, and international laws and regulations relevant to their role and World Bank's operations. This includes, but is not limited to, laws and regulations pertaining to financial services, data protection and privacy, anti-money laundering (AML), counter-terrorist financing (CTF), securities trading, and employment practices. The financial industry is highly regulated, and compliance is not optional but a fundamental requirement. *Rationale:* Ensures the Bank operates lawfully and avoids legal penalties and reputational damage.

2.13.2. Data Privacy: Personnel must handle all personal data (of customers, employees, or other individuals) in strict accordance with applicable data privacy laws (e.g., GDPR, CCPA, local equivalents) and World Bank's Data Privacy Policy. This includes respecting individuals' rights regarding their data, ensuring lawful basis for processing, and implementing appropriate security measures for personal data. *Rationale:* Protects individuals' privacy rights and ensures compliance with increasingly stringent data privacy regulations.

2.14. Security Awareness Training Participation

2.14.1. Mandatory Training: All personnel are required to complete mandatory security awareness training upon hiring and at least annually thereafter. Additional ad-hoc or role-specific security training may be assigned as deemed necessary by IT Cybersecurity or management based on evolving threats or job functions. Completion of training will be tracked. *Rationale:* Ensures all personnel have a baseline understanding of security threats, policies, and their responsibilities. Regular refreshers keep this knowledge current.

2.14.2. Phishing Simulations: Personnel are expected to participate actively in Bank-conducted phishing simulation exercises. These exercises are designed to test awareness and responsiveness to phishing attacks. Employees should apply lessons learned from these simulations to better identify and report real phishing attempts. *Rationale:* Provides practical experience in recognizing a common and dangerous attack vector.

2.14.3. Staying Informed: While the Bank provides formal training, personnel are encouraged to stay generally informed about current cybersecurity threats, common attack methods, and best practices for personal and corporate security. *Rationale:* Promotes a proactive security mindset.

2.15. Consequences of Violations

2.15.1. Disciplinary Action: Violations of this Security Code of Conduct may lead to disciplinary action by World Bank. The severity of the disciplinary action will depend on the

nature and gravity of the violation, intent, history of similar conduct, and impact or potential impact on the Bank, its customers, or employees. Disciplinary measures can range from verbal or written warnings, mandatory retraining, suspension of access privileges, to more severe actions up to and including termination of employment or contract, in accordance with applicable labor laws and Bank disciplinary procedures. *Rationale:* Clearly communicates that violations have serious employment consequences. The severe financial, reputational, and operational impacts of non-compliance with security regulations necessitate a firm stance on policy adherence.

2.15.2. Legal Liability: In addition to internal disciplinary actions, individuals whose actions violate laws or regulations, or cause significant harm or loss to the Bank or its customers through intentional misconduct or gross negligence, may be subject to personal legal liability, including civil lawsuits or criminal prosecution. *Rationale:* Informs personnel of potential personal legal risks associated with serious security breaches or illegal acts.

The non-compliance with this Security Code of Conduct can trigger direct legal and financial repercussions for both the individual employee and World Bank as an entity. This elevates the Code from a mere set of internal guidelines to a critical instrument for risk management and regulatory compliance. For example, if an employee's negligent actions in violation of this Code lead to a data breach, the Bank could face substantial fines from regulators, loss of customer trust, and significant operational disruption. Therefore, the "Consequences of Violations" section must be unambiguous and reflect these potentially severe outcomes to underscore the importance of adherence.

2.16. Acknowledgement and Agreement

All World Bank personnel will be required to read this Security Code of Conduct in its entirety, attest to their understanding of its provisions, and formally acknowledge their agreement to comply with it. This acknowledgement will be obtained upon hiring and reaffirmed on an annual basis, or whenever significant updates to the Code are made. Signed acknowledgements will be maintained by the Human Resources department. *Rationale:* Ensures and documents that all personnel are aware of and have agreed to abide by the Code.

2.17. Policy Review and Updates

This Security Code of Conduct will be reviewed at least annually by a committee comprising representatives from IT Cybersecurity, Human Resources, Legal, and Compliance departments. It will be updated as necessary to reflect changes in the cybersecurity threat landscape, evolving business operations, new technologies, amendments to laws and regulations, and best practices in information security and ethical conduct. Approved updates will be communicated to all personnel. *Rationale:* Keeps the Code relevant, effective, and aligned with the current environment.