JPMORGAN CHASE & CO.

James A. LaFleur
Managing Director
Chief Technology Controls Officer

Rohan M. Amin
Managing Director
Chief Information Security Officer

JPMorgan Chase's Program to Safeguard Customer Information and Provide a Secure Information Technology Environment

Dear Valued Customer,

At JPMorgan Chase (JPMC), we are committed to safeguarding our customers' data and have developed a rigorous program to do so. We are also committed to observing the data protection laws and regulations in each of the jurisdictions in which we do business.

Our Information Technology (IT) Risk and Security Management Program is designed to:

- Provide clear guidance regarding the protection of customer information;
- Monitor our systems for threats to customer information;
- Provide security solutions that minimize the threat to customer information;
- Help employees understand their responsibilities with respect to the protection of customer information and the security of our systems;
- Expect our relevant third-party service providers to adhere to specific security policies and standards, as well as regulatory obligations as applicable;
- Address all customer notification and other requirements regarding information protection.

The IT Risk and Security Management Program is governed by the following principles:

- The foundation of the Program is a set of IT Risk and Security Policies and Standards that establish rules for safeguarding the JPMC IT environment.
- The Program has oversight by the Global Technology Operating Committee and is managed by a firmwide Global Technology Controls Committee, composed of representatives of each line of business and relevant JPMC corporate functions.
- The Program is reviewed and approved by the JPMC Audit Committee of the Board of Directors on an annual basis.
- Our IT programs and processes are subject to reviews on an ongoing basis by JPMC internal and external Auditors.
- The Program is subject to periodic inspections by regulatory authorities across the world in countries where JPMC operates.

James A. LaFleur
Managing Director
Chief Technology Controls Officer

Rohan M. Amin
Managing Director
Chief Information Security Officer

Areas of Focus

Key areas of the JPMC IT Risk and Security Management Program are:

Application Security:
This Program component is designed to ensure that applications are developed with appropriate controls in place and that existing applications are protected against new threats as they arise. Components of the Application Security Program include:

- Application risk classification to determine the inherent risk factors and rating of each application;
- Application controls assessments to ensure that systems are developed, acquired and maintained with the appropriate technology controls;
- Regular third-party application security assessments;
- Multiple application source code scanning, including dynamic, static and open source to detect vulnerabilities, malicious code and defects before release to production;
- Application threat-based penetration testing and perimeter scanning of production web applications;
- An active vulnerability management program to expedite remediation as critical vulnerabilities are found;
- Mandatory security training and awareness for application developers.

-

Cybersecurity Operations and Threat Management:
This Program component is designed to protect the firm's technology infrastructure and to coordinate firmwide responses to security-related events. The Cybersecurity Operations and Threat Management teams view security as a coordinated and integrated effort across the firm and the external ecosystem. This strategy drives decision making across several strategic pillars:

- Security engineered into the foundational technology architecture that provides a resilient framework by adapting security and controls to global business, regulatory and threat environments;
- Innovation striving for strong security operations that are risk-based and intelligence-led, including comprehensive insider and external threat protection programs;

James A. LaFleur
Managing Director
Chief Technology Controls Officer

Rohan M. Amin
Managing Director
Chief Information Security Officer

- Full engagement of the business and the external ecosystem as cyber defense partners to enable awareness and preparedness through robust training and simulation that increase the reach of cyber defense through our global partners' engagement.

Data Protection:
This Program component is designed to ensure that appropriate controls are in place to safeguard the customer data handled by JPMC. Components of the Data Protection Program include:

- Key business data protection at every level of the organization, with a particular focus on the security of critical information and offering differential protection for critical information assets;
- Clearly identified Personal Information (PI) data elements with requirements for handling such data;
- Data Loss Prevention (DLP) controls, which help to prevent certain types of PI data from leaving JPMC in an unauthorized or unsecured manner;
- Encryption tools, which enable employees to transmit confidential data in a secure manner when authorized to do so;
- Mobile device and portable media controls, designed to prevent the unauthorized use of these devices and ensure only secured, encrypted solutions are used;
- Data retention and disposal solutions, designed to meet applicable legal and regulatory requirements for the management of customer data.

Global Identity and Access Management (GIAM):
The primary focus of the Global Identity and Access Management Program is the institution of access standards and controls across the firm's infrastructure and applications, particularly those that contain customer information. These controls include:

- Management of an end-to-end access provisioning lifecycle, requiring management approval that end user access is appropriate and ensuring the timely removal of access upon termination or a change in an end user's job responsibilities;
- A risk-based access certification program, requiring management attestation that end user access remains appropriate;
- Privileged access management tools, which are designed to further control and monitor use of privileged entitlements to prevent or detect unauthorized activity;
- Capabilities and tools to implement multifactor authentication and other advanced authentication systems where required to meet legal and regulatory requirements.

James A. LaFleur
Managing Director
Chief Technology Controls Officer

Rohan M. Amin
Managing Director
Chief Information Security Officer

IT Risk and Controls Framework Program:
The Program to maintain the firmwide IT Risk and Controls Framework includes the periodic update of Information Technology policies and standards, the technology controls assessment process and the reporting of key performance indicators. Components of the Program include:

- A body of firmwide IT risk and security policies;
- A risk assessment framework for technology environments;
- A governance and oversight process to report on key risk indicators and provide visibility into the risk posture of the firm and to prioritize issue resolution; and
- A program to manage identification of and compliance with technology legal and regulatory requirements in jurisdictions in which the firm does business.

Third-Party Technology Risk Management:
This firmwide framework is designed to identify, assess and address IT risks arising from third-party vendors and partners regarding the controls they have in place to protect JPMC as well as its customers. Components of the Third-Party Technology Risk Management Program include:

- Regular risk-based assessments of third-party providers against JPMC's IT policies and standards;
- Regular oversight of remediation of issues identified during those assessments.

Privacy

The JPMorgan Chase Privacy Program is managed by the JPMC Chief Privacy office and is designed to comply with global privacy regulatory requirements through the development of policies, standards, controls, advisory services and process enhancements. Core components of the Program include:

- A firmwide governance framework that promotes corporate responsibility and helps to manage and escalate key privacy risks;
- Oversight and guidance for lines of business and regions;
- A global privacy training and awareness program;
- A process to manage potential privacy incidents;
- Consumer privacy notices that describe how we protect privacy and offer certain choices regarding our management of consumers' personal information.

James A. LaFleur
Managing Director
Chief Technology Controls Officer

Rohan M. Amin
Managing Director
Chief Information Security Officer

Training and Awareness

Our Security Awareness Program includes ongoing updates and training that reinforce the firm's IT Risk and Security Management policies, standards and practices, as well as the expectation that employees comply with these policies. The Security Awareness Program engages personnel through live, virtual and computer-based training. The program has been enhanced to provide regular coverage on cybersecurity, phishing and securing access.

Thank you for your continued confidence in JPMorgan Chase.

James A. LaFleur
Chief Technology Controls Officer
JPMorgan Chase & Co.

Rohan M. Amin
Chief Information Security Officer
JPMorgan Chase & Co.