INFORMATION SECURITY MONITORING NOTICE

Effective: 1st May 2025

INTRODUCTION

The legal entity named on the contract of employment of the Employee, or the engagement of the Contractor (the "**Company**") has prepared this Information Security Monitoring Notice[1] (the "**Notice**") to supplement the Employee and Contractor Data Protection Notice (the "**DPN**") that you receive as an employee or contractor to set out its practices regarding the monitoring of data and other materials (including but not exclusively, business and personal[2] messages, communications and information) transmitted, received, processed and/or stored by the Company's electronic systems and devices. These include, but are not limited to, network, voice, computer, company issued mobile devices, instant messaging, web applications, mobile applications, social media, audio conferencing, video conferencing and fax infrastructure ("**Electronic Communications**"), printer use, the Internet, and physical access logs.

This Notice applies to all individuals or groups that have been provided with access to the Company's systems, facilities and/or information for a business purpose or supervisory function, including employees, consultants, contractors, non-executive directors and other workers in the Company (each an "**Authorized User**"). Appendix A sets out a non-exhaustive list of the communications and records which we monitor and from which we may collect any individually identifiable information on Authorized Users ("**Personal Data**") and the purposes for which we may use, transfer and disclose Personal Data.

Authorized Users who require this Notice in a language other than those provided should contact Global Information Security using the information set out in the Contact Details section. In the event this Notice is provided to an Authorized User in a language other than English, any discrepancy, conflict or inconsistency between the two language versions shall be resolved as set out in the relevant DPN.

Irrespective of location, monitoring tools and processes are routinely deployed by the Company to the Company's electronic systems and devices to the extent not prohibited under local laws or regulations. All monitoring activity that takes place on the Company's electronic systems and devices is conducted in accordance with this Notice.

Any Personal Data collected (directly or indirectly) in the course of the monitoring processes will be treated in accordance with the relevant DPN as issued from time to time. The processing of Personal Data is carried out with the aid of manual and electronic tools.

This Notice references key portions of relevant policies of the Company, but does not contain all of the Company's policies and requirements applicable to the use of Electronic Communications and the Internet. Authorized Users are required to comply with the requirements noted in the Company's Code of Conduct, Electronic Communications Guide and the Global Information Security Policy documents, as well as any

[1] The Information Security Monitoring Notice (ISMN), was previously titled The Cyber Security Monitoring Notice (CSMN) and may also be referred to as such in other company documentation

[2] In line with the Code of Conduct, Authorized Users are permitted limited personal use of company managed devices and applications, the internet and email for personal communications. The use of the resources may be monitored and inspected to maintain the integrity of the systems (e.g., monitoring for the introduction of malware or inappropriate data transmissions) and avoid activities that may give rise to company liability or risk.

other applicable standards issued by the Company from time to time. All capitalized terms used but not defined in this Notice shall have the meanings assigned to them in the Company's Global Information Security Policy documents.

Communications by certain regulated Company personnel are subject to additional detailed supervisory requirements and Authorized Users are reminded to consult the relevant policies and procedures for their line of business for further information.

Subject to applicable law, all Electronic Communications, including emails (encrypted[3] and unencrypted) and connections to the Internet and intranet websites using Company computing or network resources are the property of the Company and may be subject to monitoring and surveillance. This includes but is not limited to:

- **Conducting monitoring activities without giving prior notice ("covert monitoring"), in circumstances where it is permitted to do so (for example where it has suspicions of data exfiltration, criminal or other unlawful activities or breach of the Company's Compliance or Global Information Security Policies or breach of any other obligation owed to the Company) or, where required under applicable law, under a relevant warrant or authorization;**
- **Monitoring and/or blocking of inbound and outbound emails and other messaging marked to indicate that they are personal or private or otherwise of a personal nature where it has a suspicion that such emails and their contents or attachments contravene or breach applicable law or Company's Compliance or Global Information Security Policies or any other obligation owed to the Company.**

PERSONAL DATA COLLECTION AND PURPOSES OF USE

Certain monitoring activities of the Company's electronic systems and devices are practiced throughout the Company for the purposes set out in Appendix A of this Notice.

The categories of Personal Data that the Company may process whilst undertaking the monitoring outlined in this Notice and the legal grounds for such processing (including consent, where necessary) are as set out in the relevant DPN.

Authorized Users may have additional rights. Rights of Individuals, subject to applicable law, are set out in the relevant DPN. (Section VII: Access, Portability, Rectification and Suppression, Limitation and Restriction of Processing and Accuracy of Personal Data).

The Company reserves the right, subject to applicable law and without further notice, to deploy enhanced data monitoring on your bank provided computer and/or mobile device in certain circumstances (including but not limited to you having elevated privileges, elevated access, or an approaching departure date).

3 Where the monitoring and surveillance of encrypted communications involves the breaking and re-application of encryption.

SENSITIVE PERSONAL DATA

The Company may collect and process certain special categories of Personal Data including Sensitive Personal Data as set out in the relevant DPN in the course of conducting the activities described in this Notice.

Global Information Security monitoring activities do not actively monitor for Sensitive Personal Data, however some Sensitive Personal Data may inevitably be disclosed during monitoring for other types of data.

ACCESS BY COMPANY PERSONNEL

Access to personal data processed pursuant to this notice is restricted to those individuals who need such access for the purposes listed in the relevant DPN including but not limited to members of the Global Information Security team and Internal Enterprise Investigations in an Authorized User's home jurisdiction and/or other jurisdictions in which the Company has operations.

DISCLOSURE

The monitoring tools and processes described in this Notice may be deployed by the Global Information Security teams of the Company and any of its affiliates and branches including those located in the U.S., the U.K., Singapore, Hong Kong and India as well as within the specific country/region of operation. Personal Data may be stored and/or processed in an Authorized Users home jurisdiction and/or other jurisdictions in which the Company has operations.

Given the global nature of the Company's activities, the Company may therefore transfer your Personal Data to countries located outside of your home country, as set out in the relevant DPN.

The Company may disclose, in accordance with applicable law, relevant Personal Data to any of its affiliates, and branches and they may process such Personal Data for the purposes set out in this Notice. In addition, the Company may disclose, in accordance with applicable law, relevant Personal Data to certain third parties as set out in relevant DPN.

SECURITY

The Company maintains appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of or damage to Personal Data.

MODALITIES OF THE PROCESSING AND DATA RETENTION

All monitoring and surveillance activities are initially non-individualised, and only target a specific Authorized User if there are signs of abuse or irregular behaviour, for the purposes set out in this Notice. In the event personal use of bank systems results in a personal communication that requires review, any review will be undertaken in line with applicable laws, rules and regulations.

In processing Personal Data for the purposes set out in this Notice, the Company does not use automated decision making on Authorized User processes where the decision would have a legal or similarly significant effect on the Authorized User when conducting monitoring as described in this Notice. 'Automated decision making' is the process of making a decision by automated means without any human involvement.

The retention periods for each type of data and jurisdiction are outlined on the Global Records Retention Schedule found on the Global Records Management page on Flagscape. Retention requirements are available upon request for new Authorized Users who do not yet have access to the internal site. The Company will delete Personal Data after the applicable retention period.

DISCIPLINARY ACTION

Authorized Users who violate any of the policies referenced in this Notice may be subject to investigation, suspension of access and/or disciplinary proceedings (up to and including termination of employment or contract services). Authorized Users who are not employees may be subject to referral to their employer for disciplinary action. Authorized Users who violate applicable laws or regulations may be referred to law enforcement and/or regulatory officials in accordance with legal and regulatory requirements. Any material or evidence identified via (including but not limited to) the monitoring of telephone calls, emails and Internet or intranet use (including personal telephone calls, emails and Internet usage) may be relied upon in any disciplinary proceedings and internal or external investigations. Authorized Users are expected to cooperate in inquiries, inspections, monitoring and recording activities if asked. Refusing to cooperate with a security investigation may result in legal or disciplinary action, including termination of employment or contract services.

CONTACT DETAILS

For questions or more information about this Notice or Global Information Security monitoring activities, Authorized Users should contact Global Information Security.

You may have the right to lodge a complaint with the Data Protection Authority for your country, for applicability and further information refer to the relevant DPN.

For questions regarding local laws and restrictions, Authorized Users should contact their local compliance officer, Data Protection Officer or legal department.

CHANGES TO THIS NOTICE

This Notice is not contractual and the Company reserves the right to modify or withdraw the Notice at any time. Should the Company make substantial changes to this Notice, it will notify Authorized Users as soon as reasonably possible by reissuing a revised Notice and/or taking other steps in accordance with applicable laws.

APPENDIX A

Refer to the matrix linked here to view the categories of data that may be collected for each purpose of use, summarized below. The matrix is available upon request for new Authorized Users who do not yet have access to the internal site.

The Communications and Records (both live and after the event) which we monitor on the Company's electronic systems and devices and from which we may collect Personal Data include, but are not limited to:

- Emails sent;
- Emails received;
- Web / internet usage, FTP, HTTP, HTTPS, Telnet;
- Print usage and content;
- Files located on desktop (outside My Documents), collaboration sites, open shares, internal Wiki's;
- Removable media, Non-Company managed devices connecting to Company system;
- Instant messaging;
- Telephone calls, VOIP calls, voicemails;
- Application access and usage logs and records;
- Network access information (including IP address and ISP);
- System access and usage logs and records (including records showing course of usage and conduct);
- Fax & Document Scanning/Imaging;
- Social media usage and content (external, non-Company);
- Open source and publicly available information;
- Security logs;
- Key logs and screen shots;
- Conferencing technologies;
- Cookies, Beacons, Sinkholes and Honeypots;
- Geolocation Data[4]
- Swipe Card entry data;
- Text Messages sent and received.

THE PURPOSES FOR WHICH WE MAY COLLECT, USE, TRANSFER AND DISCLOSE PERSONAL DATA:

The Global Information Security Policy is designed to provide the necessary requirements to enable the Company to prepare, prevent, detect, respond and recover from increasing changes in the threat landscape. The Global Information Security Program provides solutions and uses advanced techniques to prevent information security threats from undermining customer confidence and disrupting business operations. Global Information Security protects the Company and its clients by using a risk-based and outcome-focused

[4] Geolocation data is defined as data taken from a user's device which indicates the geographical location of that device, including GPS data or data about connection with local wifi equipment

framework.

- Prepare: We protect by continually updating the Information Security Programme, which includes complying with local or foreign state and/or country specific laws to better anticipate and identify potential threats;
- Prevent: We protect by staying ahead of adversaries through the deployment of preventative controls to prevent loss, misuse and inappropriate use of confidential and proprietary information and reduce the number of incidents;
- Detect: We protect by limiting exposure through the deployment of detective controls including firewall monitoring, anti-spam and virus protection, and other monitoring; continuously monitoring all bank teammates, applications, data, systems and networks;
- Mitigate: We protect by mitigating incidents through an agile and coordinated response capability;
- Respond/Recover: We protect by improving security posture through robust forensics, investigations, and lessons learned capability while addressing any compliance issues, regulatory inquiries, disciplinary actions, or legal claims

信息安全监测通知

生效日期：2025 年 5 月 1 日

引言

本信息安全监测通知[5]（“**通知**”）由员工雇佣合同或承包商聘用合同上提及的法人实体（“**本公司**”）拟定，以对您作为员工或承包商收到的《员工与承包商数据保护通知》（“**DPN**”）进行补充，在有关公司电子系统和设备传输、接收、处理和/或存储的数据和其他材料（包括但不仅限于业务和个人[6]消息、通信和信息）监测方面规范其行为。这些电子系统和设备包括但不限于网络、语音、电脑、本公司发放的移动设备、即时通讯、网络应用程序、社交媒体、音频会议技术、视频会议技术和传真基础设施（“**电子通信**”）、打印机的使用、互联网和物理访问日志。

本通知适用于因业务目的或监管职能而获权访问本公司系统、设施和 / 或信息的所有个人或团队，包括公司的员工、顾问、承包商、非执行董事和其他工人（每名人士均为“**授权用户**”）。附录 A 中列明的非穷尽列表包含我们监测且可能从中收集授权用户身份信息（“**个人数据**”）的通信和记录，并且列明了我们使用、传输和披露个人数据的目的。

需要以所提供语言以外的其他语言获取本通知的授权用户应使用“联系方式”部分中列出的信息联系全球信息安全部。若本通知以英文以外的其他语言提供给授权用户，那么两种语言版本之间的任何差异、冲突或不一致应按照相关 DPN 中规定的方式予以解决。

在当地法律或法规未禁止的范围内，无论地点如何，监测工具和流程由本公司日常部署到公司的电子系统和设备中。对本公司的电子系统和设备采取的所有监测活动皆根据本通知进行。

在监测过程中收集的任何个人数据将根据不时发布的相关 DPN 进行处理。个人数据的处理在手动和电子工具的辅助下进行。

本通知参考本公司相关政策的关键部分，但不包含适用于电子通信和互联网使用的所有本公司政策和要求。授权用户须遵守本公司的《行为准则》、《电子通信指南》以及《全球信息安全政策文件》中载明的要求，以及遵守本公司不时发布的任何其他适用标准。本通知中使用但未定义的所有术语应拥有本公司的全球信息安全政策文件 (Global Information Security Policy documents) 中赋予的含义。

部分受监管的本公司人员的通信受其他详细的监管要求所规限，且会提醒授权用户就其业务范围查阅相关政策和程序，以了解更多信息。

---

[5]信息安全监测通知 (ISMN) 以前被称为“网络安全监测通知”(CSMN)，在本公司其他文件中也可能使用该旧名

[6]根据《行为准则》，允许授权用户将银行管理设备和应用程序用于有限的个人用途，将互联网和电子邮箱用于个人通信。对资源的使用情况可能受到监控和检查，以保持系统完整性（例如监控恶意软件侵入或不当数据传输），并避免可能使本公司承担责任或风险的活动。

视适用法律规定，所有电子通信[包括使用本公司计算或网络资源的电子邮件（加密[7]和未加密）以及互联网和内部网网站连接]均属于本公司的财产并可能受到监测和监督。这包括但不限于：

- **在允许的情况下，或者在适用法律要求时根据相关的许可或授权，无需事先发出通知即可开展监测活动（"秘密监测"）（例如，若怀疑存在数据外泄、犯罪或其他违法活动，或违反本公司合规或全球信息安全政策的行为，或者违反对本公司所负有的任何其他义务的行为）；**
- **监测和/或拦截入站和出站电子邮件以及其他标记为个人或私密或其他私人性质的消息传送，若其怀疑此类电子邮件及其内容或附件违反适用法律、本公司合规或全球信息安全政策，或违反对本公司所负有的任何其他义务。**

个人数据收集和使用目的

本公司已出于本通知附录 A 所载列的目的在全公司对本公司的电子系统和设备实行某些监测活动。

本公司在进行本通知所概述的监测工作时可能处理的个人数据类别，以及此类处理（如有需要，包括同意）的法律依据载于相关 DPN 中。

授权用户可能拥有其他权利。个人的权利（受适用法律规限）载于相关 DPN 中。（第 VII 部分：访问、可移植性、纠正和抑制、处理限制和约束以及个人数据的准确性）。

在特定的情况下（包括但不限于您拥有更高的特权、更高的访问权限或即将到来的出发日期），本公司保留在遵守适用法律且不另行通知的情况下，在您的银行提供的计算机和/或移动设备上部署增强数据监控的权利。

敏感个人数据

本公司在开展本通知所述的活动期间，可收集和处理相关 DPN 中列明的某些特殊类别的个人数据（包括敏感个人数据）。

全球信息安全监测活动不主动监测敏感个人数据，但在监测其他类型的数据时，一些敏感个人数据不可能避免地遭到披露。

本公司员工的访问权限

根据本通知处理的个人数据的访问权限，仅限于出于相关 DPN 中所列目的需要此类访问权限的个人，包括但不限于全球信息安全团队成员和获得授权用户所在司法管辖区和/或本公司开展运营活动所在地的其他司法管辖区的内部企业调查人员。

---

7 加密通信的监测和监控涉及加密的破坏和重新应用。

信息披露

本通知所述的监测工具和流程可由本公司及其在美国、英国、新加坡、中国香港和印度以及运营所在的特定国家/地区设立的任何关联公司和分公司的全球信息安全团队部署。个人数据可能在授权用户的原属司法管辖区和/或本公司经营业务所在地的其他司法管辖区存储和/或处理。

鉴于本公司活动的全球性质，本公司可按照相关 DPN 中的规定，将您的个人数据传输到您母国以外的国家/地区。

本公司可依据适用法律向其任何关联方和分支机构披露相关个人数据，且可出于本通知中所列的目的处理此类个人数据。此外，本公司可依据适用法律，向相关 DPN 中列明的特定第三方披露相关个人数据。

安全性

本公司维持合适的技术和组织措施，以防止未经授权或非法处理个人数据，和/或防止个人数据意外丢失、篡改、披露或访问、意外或非法销毁或破坏。

处理形式和资料保留

所有监测和监控活动最初均不指向具体个人，仅在出现滥用或异常行为迹象时，出于本通知中规定的目的针对具体的授权用户。如果个人使用银行系统导致需要审查私人通信，则将根据适用法律、规则和法规进行任何审查。

在出于本通知规定目的处理个人数据时，如果实施本通知描述的监测会对授权用户产生法律或类似的重大影响，本公司不会对授权用户流程使用自动化决策。“自动化决策”是在没有人干预的情况下通过自动化的方法进行决策的流程。

每种数据和司法管辖区的保留期限在全球记录保留计划中列明，该表可在 Flagscape 的全球记录管理页面上找到。尚未获得互联网访问权限的新授权用户在提出要求后可以获取该保留要求。本公司将在适用保留期限结束后删除个人数据。

纪律处分

违反本通知所引用任何政策的授权用户可能会遭受调查、暂停使用权和/或按纪律处分程序处理（最高处分包括终止雇佣或承包服务）。非员工授权用户可能会被转交予其雇主进行纪律处分。依据法律和监管要求，违反适用法律或法规的授权用户可能会被转交予执法机关和/或监管官员。通过（包括但不限于）监测电话通话、电子邮件和互联网或内部网使用（包括私人电话通话、电子邮件和互联网使用）而发现的任何材料或证据可能会成为任何纪律处分程序和内部或外部调查的依据。授权用户应配合开展调查、检查、监测和记录活动（如被要求）。拒绝配合安全调查可能会招致法律或纪律处分，包括终止雇佣或承包服务。

联系信息

有關本通知或全球資訊安全監控活動的問題或更多資訊，授權使用者應聯繫全球資訊安全。

您有权向您所在国家/地区的数据保护机关提起申诉，对于适用性和进一步的信息，请参考相关 DPN。

如对本地法律和限制存有疑问，获授权用户应联系其所在地的合规官、数据保护专员或法律部。

本通知的变更

本通知并非合同，且本公司保留随时修改或撤销通知的权利。若本公司对本通知进行了重大变更，将根据适用法律，重新发布修订后的通知和/或采取其他步骤，尽快通知授权用户。

附录 A

参见此处链接的矩阵，以查看以下可能为了各种用途之目的收集的数据类型综述。还没有获得互联网访问权限的新授权用户在提出要求后可以获取该矩阵。

我们在本公司的电子系统和设备上监测及可能收集个人数据的通信和记录（包括现场及事后）包括但不限于：

- 电子邮件已发送；
- 电子邮件已接收；
- 网页/互联网使用、FTP、HTTP、HTTPS、Telnet；
- 打印用途和内容；
- 文件位于桌面（“我的文档”外面）、合作网站、开放共享、内部 Wiki；
- 连接至本公司系统的可移动媒介、非银行管理设备；
- 即时消息；
- 电话通话、VOIP 通话、语音邮件；
- 应用程序访问和使用日志与记录；
- 网络访问信息（包括 IP 地址和 ISP）；
- 系统访问和使用日志与记录（包括显示使用和执行过程的记录）；
- 传真和文档扫描/映像；
- 社交媒体的使用和内容（外部，非本公司）；
- 开源和公开发布的信息；
- 安全日志；
- 密钥日志和屏幕截图；
- 会议技术；
- Cookie、Beacon、Sinkhole 和 Honeypot；
- 地理位置数据[8]

[8] 地理位置数据是指从用户设备中获取的数据，用于指示该设备的地理位置，包括 GPS 数据或与本地 wifi 设备连接的数据

- 磁卡录入数据；
- 发送和接收的短信。

我们可能收集、使用、传输和披露个人数据的目的：

本全球信息安全政策旨在提供必要的要求，使本公司能够准备、预防、探测、应对威胁局面下不断增加的变化并从中恢复。全球信息安全计划提供了解决方案，并利用先进技术来防止信息安全威胁破坏顾客信心以及干扰业务运营。全球信息安全计划采用一种基于风险、注重结果的框架，保障本公司及其客户的安全。

- 准备：我们通过持续更新信息安全计划提供保护，其中包括遵守当地或其他州和/或国家的具体法律，以更好地预测和识别潜在威胁；
- 预防：我们通过部署预防性控制措施，防止机密和专有信息的丢失、滥用和不当使用，减少事故数量，比竞争对手抢先一步占据先机，从而提供保护；
- 检测：我们通过部署检测控制措施（包括防火墙监测、反垃圾邮件和病毒保护以及其他监测等）限制暴露，持续监测所有银行同事、应用程序、数据、系统和网络，从而提供保护；
- 规避：我们通过敏捷的协作型响应能力规避事故，从而提供保护；
- 响应/恢复：我们通过强大的鉴证、调查以及经验汲取能力提升安全态势，同时解决任何合规问题、监管质询、纪律处分或法律索赔，从而提供保护。

PEMBERITAHUAN PEMANTAUAN KEAMANAN INFORMASI

Berlaku: 1 Mei 2025

PENDAHULUAN

Badan hukum yang disebutkan dalam kontrak kerja Karyawan, atau perjanjian Kontraktor ("Perusahaan") telah menyiapkan Pemberitahuan Pemantauan Keamanan Informasi ini[9] ("**Pemberitahuan**") untuk melengkapi Pemberitahuan Perlindungan Data Karyawan dan Kontraktor (Data Protection Notice/"**DPN**") yang Anda terima sebagai karyawan atau kontraktor untuk menetapkan praktiknya mengenai pemantauan data dan materi lainnya (termasuk namun tidak terbatas pada, pesan, komunikasi, dan informasi bisnis maupun pribadi[10]) yang dikirimkan, diterima, diproses dan/atau disimpan oleh sistem dan perangkat elektronik Perusahaan. Ini termasuk, tetapi tidak terbatas pada, jaringan, suara, komputer, perangkat seluler yang disediakan perusahaan, perpesanan instan, aplikasi web, aplikasi seluler, media sosial, infrastruktur konferensi, konferensi video, dan faks ("**Komunikasi Elektronik**"), penggunaan printer, Internet, dan log akses fisik.

Pemberitahuan ini berlaku untuk semua individu atau kelompok yang telah diberi akses ke sistem, fasilitas, dan/atau informasi Perusahaan untuk kepentingan bisnis atau fungsi pengawasan, termasuk karyawan, konsultan, kontraktor, direktur noneksekutif, dan pekerja lain di Perusahaan (masing-masing disebut "**Pengguna Resmi**"). Lampiran A menjabarkan daftar tidak lengkap komunikasi dan catatan yang kami pantau dan yang menjadi sumber kami dalam pengumpulan informasi pengidentifikasi individu tentang Pengguna Resmi ("**Data Pribadi**") serta tujuan penggunaan, pengalihan, dan pengungkapan Data Pribadi oleh kami.

Pengguna Resmi yang memerlukan Pemberitahuan ini dalam bahasa selain yang disediakan harus menghubungi bagian Keamanan Informasi Global dengan menggunakan informasi yang ditetapkan di bagian Detail Kontak. Apabila Pemberitahuan ini disediakan untuk Pengguna Resmi dalam bahasa selain bahasa Inggris, segala ketidakcocokan, perbedaan, atau ketidaksesuaian antara kedua versi bahasa tersebut akan diselesaikan sebagaimana ditetapkan dalam DPN yang relevan.

Terlepas dari lokasi, alat dan proses pemantauan disebarkan secara rutin oleh Perusahaan pada sistem dan perangkat elektronik Perusahaan sejauh tidak dilarang oleh hukum atau peraturan setempat. Semua aktivitas pemantauan yang terjadi pada sistem dan perangkat elektronik perusahaan dilaksanakan sesuai dengan Pemberitahuan ini.

---

[9] Pemberitahuan Pemantauan Keamanan Informasi (Information security Monitoring Notice/ISMN), sebelumnya berjudul Pemberitahuan Pemantauan Keamanan Dunia Maya (Cyber Security Monitoring Notice/CSMN) dan juga dapat memiliki judul tersebut pada dokumen perusahaan lainnya

[10] Sesuai dengan Pedoman Perilaku, Pengguna Resmi diizinkan untuk menggunakan perangkat dan aplikasi yang dikelola perusahaan untuk tujuan pribadi yang terbatas, serta internet dan email untuk komunikasi pribadi. Penggunaan sumber daya tersebut dapat dipantau dan diinspeksi untuk menjaga integritas sistem (misalnya memantau penyebaran malware atau transmisi data yang tidak patut), serta menghindari aktivitas yang dapat menimbulkan liabilitas atau risiko bagi perusahaan.

Setiap Data Pribadi yang dikumpulkan (secara langsung atau tidak langsung) selama proses pemantauan akan diperlakukan sesuai dengan DPN yang relevan yang diterbitkan dari waktu ke waktu. Pemrosesan Data Pribadi dilaksanakan dengan bantuan alat bantu manual dan elektronik.

Pemberitahuan ini menyebutkan bagian utama dari kebijakan Perusahaan yang relevan, tetapi tidak berisi semua kebijakan dan persyaratan Peruahaan yang berlaku untuk penggunaan Komunikasi Elektronik dan Internet. Pengguna Resmi diwajibkan untuk mematuhi persyaratan yang tertera dalam Pedoman Perilaku, Panduan Komunikasi Elektronik, dan dokumen Kebijakan Keamanan Informasi Global Perusahaan, serta semua standar lain yang berlaku yang diterbitkan oleh Perusahaan dari waktu ke waktu. Semua istilah dalam huruf besar yang digunakan tetapi tidak dijelaskan dalam Pemberitahuan ini memiliki arti sebagaimana sudah ditetapkan untuk istilah tersebut dalam dokumen Kebijakan Keamanan Informasi Global Perusahaan.

Komunikasi yang dilakukan oleh personel Perusahaan tertentu yang diatur tunduk pada persyaratan pengawasan tambahan yang lengkap dan Pengguna Resmi diingatkan untuk mempelajari kebijakan dan prosedur yang relevan untuk mendapatkan informasi lebih jauh terkait lini bisnis mereka.

Tunduk pada hukum yang berlaku, semua Komunikasi Elektronik, termasuk email (terenkripsi[11] maupun tidak terenkripsi) dan koneksi ke Internet dan situs web intranet yang menggunakan komputasi atau sumber daya jaringan Perusahaan adalah milik Perusahaan serta dapat dipantau dan diawasi. Hal mencurigakan termasuk tapi tidak terbatas pada:

- **Melakukan aktivitas pemantauan tanpa memberikan pemberitahuan sebelumnya ("pemantauan terselubung"), dalam kondisi ketika diizinkan melakukannya (misalnya ketika ada kecurigaan yang kuat mengenai eksfiltrasi data, tindak pidana atau aktivitas pelanggaran hukum lainnya atau pelanggaran terhadap Kebijakan Kepatuhan atau Kebijakan Keamanan Informasi Global Perusahaan atau pelanggaran terhadap kewajiban lainnya kepada Perusahaan) atau, jika diharuskan oleh hukum yang berlaku, berdasarkan perintah atau kewenangan yang relevan;**
- **Memantau dan/atau memblokir email masuk dan keluar dan perpesanan lainnya yang ditandai sebagai milik pribadi atau yang bersifat pribadi di mana terdapat kecurigaan bahwa email tersebut dan isi atau lampirannya bertentangan atau melanggar hukum yang berlaku atau Kebijakan Kepatuhan atau Kebijakan Keamanan Informasi Global Perusahaan atau kewajiban lainnya kepada Perusahaan.**

PENGUMPULAN DATA PRIBADI DAN TUJUAN PENGGUNAAN

Aktivitas pemantauan tertentu terhadap sistem dan perangkat elektronik Perusahaan diterapkan di seluruh Perusahaan untuk kepentingan sebagaimana dijelaskan dalam Lampiran A Pemberitahuan ini.

Kategori Data Pribadi yang dapat diproses pihak Perusahaan saat menjalankan pemantauan sebagaimana dijelaskan dalam Pemberitahuan ini dan dasar hukum untuk melakukan pemrosesan tersebut (termasuk

11 Apabila pemantauan dan pengawasan komunikasi terenkripsi melibatkan pemutusan dan penerapan ulang enkripsi.

persetujuan, jika diperlukan) diatur dalam DPN yang relevan.

Pengguna Resmi mungkin memiliki hak tambahan. Hak Individu, sesuai dengan hukum yang berlaku, ditetapkan dalam DPN yang relevan. (Bagian VII: Akses, Portabilitas, Perbaikan dan Supresi, Pembatasan dan Pelarangan Pemrosesan serta Keakuratan Data Pribadi).

Sesuai hukum yang berlaku dan tanpa pemberitahuan lebih lanjut, Perusahaan berhak untuk mengerahkan pemantauan data yang ditingkatkan pada komputer dan/atau perangkat seluler yang disediakan bank Anda dalam keadaan tertentu (termasuk namun tidak terbatas pada Anda yang memiliki hak istimewa yang ditingkatkan, akses yang ditingkatkan, atau tanggal keberangkatan yang mendekati).

DATA PRIBADI SENSITIF

Perusahaan dapat mengumpulkan dan memproses kategori khusus Data Pribadi tertentu termasuk Data Pribadi Sensitif, sebagaimana diatur dalam DPN yang relevan, selama melaksanakan aktivitas yang disebutkan dalam Pemberitahuan ini.

Aktivitas pemantauan Keamanan Informasi Global tidak secara aktif memantau Data Pribadi sensitif, tetapi beberapa Data Pribadi Sensitif dapat diungkapkan selama pemantauan jenis data lain.

AKSES OLEH PERSONEL PERUSAHAAN

Akses ke data pribadi yang diproses sesuai dengan pemberitahuan ini dibatasi bagi individu yang memerlukan akses tersebut untuk tujuan yang tercantum dalam DPN terkait, termasuk, namun tidak terbatas pada anggota tim Keamanan Informasi Global dan Penyelidikan Perusahaan Internal di yurisdiksi asal Pengguna Resmi dan/atau yurisdiksi lain tempat Perusahaan beroperasi.

PENGUNGKAPAN

Alat bantu dan proses pemantauan yang dijelaskan dalam Pemberitahuan ini bisa diluncurkan oleh tim Keamanan Informasi Global Perusahaan dan afiliasi dan cabang mana pun termasuk yang berlokasi di AS, Britania Raya, Singapura, Hong Kong, dan India serta yang berada di negara/wilayah operasi tertentu. Data Pribadi dapat disimpan dan/atau diproses di yurisdiksi asal Pengguna Resmi dan/atau yurisdiksi lain tempat Perusahaan beroperasi.

Karena sifat global dari aktivitas Perusahaan, maka Perusahaan dapat mengalihkan Data Pribadi Anda ke luar negara asal Anda, sebagaimana diatur dalam DPN yang relevan.

Sesuai dengan hukum yang berlaku, Perusahaan dapat mengungkapkan Data Pribadi yang relevan ke semua afiliasi dan cabangnya, dan mereka dapat memproses Data Pribadi tersebut untuk tujuan sebagaimana diatur dalam Pemberitahuan ini. Selain itu, sesuai hukum yang berlaku, pihak Perusahaan dapat mengungkapkan Data Pribadi yang relevan ke pihak ketiga tertentu yang diatur dalam DPN yang relevan.

KEAMANAN

Perusahaan menegakkan langkah teknis dan organisasi yang sesuai untuk memberikan perlindungan

terhadap pemrosesan Data Pribadi tanpa izin atau tidak sah dan/atau kehilangan, perubahan, pengungkapan atau akses, atau pemusnahan atau kerusakan Data Pribadi secara tidak sengaja atau tidak sah.

MODALITAS PEMROSESAN DAN PENYIMPANAN DATA

Semua aktivitas pemantauan dan pengawasan pada awalnya bersifat non-individu, dan hanya menargetkan Pengguna Resmi tertentu jika terdapat tanda-tanda penyalahgunaan atau perilaku tidak wajar, untuk tujuan yang ditetapkan dalam Pemberitahuan ini. Apabila penggunaan sistem bank secara pribadi menghasilkan komunikasi pribadi yang memerlukan peninjauan, peninjauan apa pun akan dilakukan sesuai dengan undang-undang, aturan, dan regulasi yang berlaku.

Dalam memproses Data Pribadi untuk tujuan yang ditetapkan dalam Pemberitahuan ini, Perusahaan tidak menggunakan pengambilan keputusan otomatis pada proses Pengguna Resmi atau Kontraktor yang mana keputusan tersebut akan memiliki dampak hukum atau dampak signifikan serupa terhadap Pengguna Resmi saat melaksanakan pemantauan sebagaimana dijelaskan dalam Pemberitahuan ini. Pembuatan keputusan otomatis adalah proses untuk membuat keputusan secara otomatis tanpa campur-tangan manusia.

Periode retensi untuk tiap jenis data dan yurisdiksi diuraikan dalam Daftar Retensi Dokumen Global yang dapat ditemukan pada halaman Pengelolaan Catatan Global di Flagscape. Persyaratan retensi tersedia apabila diminta bagi Pengguna Resmi baru yang belum memiliki akses pada situs internal. Perusahaan akan menghapus Data Pribadi setelah berakhirnya periode penyimpanan yang berlaku.

TINDAKAN DISIPLINER

Pengguna Resmi yang melanggar salah satu kebijakan yang dirujuk dalam Pemberitahuan ini dapat dikenakan investigasi, penangguhan akses, dan/atau proses pendisiplinan (hingga dan termasuk pemutusan hubungan kerja atau layanan kontrak). Pengguna Resmi yang bukan karyawan akan dilaporkan kepada atasan mereka agar mendapatkan tindakan pendisiplinan. Pengguna Resmi yang melanggar undang-undang atau peraturan yang berlaku dapat dilaporkan kepada petugas penegak hukum dan/atau pengawas peraturan sesuai dengan persyaratan hukum dan peraturan. Setiap materi atau bukti yang diidentifikasi melalui (termasuk tetapi tidak terbatas pada) pemantauan panggilan telepon, email dan Internet, atau penggunaan intranet (termasuk panggilan telepon pribadi, email, dan penggunaan Internet) dapat dipakai di setiap proses pendisiplinan dan investigasi internal maupun eksternal. Pengguna Resmi diharapkan untuk bekerja sama dalam aktivitas penyelidikan, inspeksi, pemantauan, dan pencatatan jika diminta. Menolak bekerja sama dalam proses investigasi keamanan dapat mengakibatkan tindakan hukum atau pendisiplinan, termasuk pemutusan hubungan kerja atau layanan kontrak.

DETAIL KONTAK

Untuk pertanyaan dan informasi lebih lanjut mengenai Pemberitahuan ini atau aktivitas pemantauan Keamanan Informasi Global, Pengguna Resmi dapat menghubungi Keamanan Informasi Global.

Anda berhak untuk mengajukan keluhan kepada Otoritas Perlindungan Data di negara Anda, dan untuk keberlakuan dan informasi lebih lanjut, lihat DPN yang relevan.

Untuk mengajukan pertanyaan tentang undang-undang dan pembatasan lokal, Pengguna Resmi harus menghubungi petugas kepatuhan, Petugas Perlindungan Data, atau departemen hukum setempat.

PERUBAHAN ATAS PEMBERITAHUAN INI

Pemberitahuan ini bukan merupakan kontrak dan Perusahaan berhak untuk mengubah atau menarik Pemberitahuan ini sewaktu-waktu. Apabila pihak Perusahaan melakukan perubahan substansial terhadap Pemberitahuan ini, maka Bank akan memberi tahu Pengguna Resmi sesegera mungkin dengan menerbitkan kembali Pemberitahuan yang telah direvisi dan/atau mengambil langkah lain yang sesuai dengan hukum yang berlaku.

LAMPIRAN A

Baca matriks yang ditautkan di sini untuk melihat berbagai kategori data yang dapat dikumpulkan untuk masing-masing tujuan penggunaan, yang dirangkum di bawah ini. Matriks dapat diberikan atas permintaan untuk Pengguna Resmi baru yang belum memiliki akses ke situs internal.

Komunikasi dan Catatan (baik pada saat maupun setelah kejadian) yang kami pantau pada sistem dan perangkat elektronik Perusahaan dan yang merupakan sumber dari mana kami mengumpulkan Data Pribadi, termasuk tetapi tidak terbatas pada:

- Email terkirim;
- Email diterima;
- Penggunaan web / internet, FTP, HTTP, HTTPS, Telnet;
- Penggunaan dan konten cetak;
- Berkas yang tersimpan di dekstop (di luar My Documents), situs kolaborasi, sumber daya terbuka, Wiki internal;
- Media yang dapat dilepas, peranti yang dikelola pihak Non-Perusahaan yang terkoneksi dengan sistem Perusahaan;
- Perpesanan instan;
- Panggilan telepon, panggilan VOIP, surat suara;
- Akses aplikasi serta log dan catatan penggunaan;
- Informasi akses jaringan (termasuk alamat IP dan ISP);
- Akses sistem serta log dan catatan penggunaan (termasuk catatan yang menunjukkan lamanya pemakaian dan penggunaannya);
- Pemindaian/pencitraan Faks & Dokumen;
- Penggunaan dan isi media sosial (eksternal, Non-Perusahaan);
- Informasi sumber terbuka dan yang tersedia secara publik;
- Log keamanan;
- Log utama dan tangkapan layar;
- Teknologi konferensi;
- Cookie, Beacon, Sinkhole, dan Honeypot;

- Data Geolokasi[12]
- Data entri Kartu Gesek;
- Pesan Teks yang dikirim dan diterima.

TUJUAN KAMI MENGUMPULKAN, MENGGUNAKAN, MENGALIHKAN, DAN MENGUNGKAPKAN DATA PRIBADI:

Kebijakan Keamanan Informasi Global dirancang untuk memberikan persyaratan yang diperlukan agar Perusahaan dapat mempersiapkan, mencegah, mendeteksi, merespons, dan memulihkan dari peningkatan perubahan dalam lanskap ancaman. Program Keamanan Informasi Global memberikan solusi dan menggunakan teknik-teknik canggih untuk mencegah ancaman keamanan informasi dari merusak kepercayaan pelanggan dan mengganggu operasi bisnis. Keamanan Informasi Global melindungi Perusahaan dan kliennya dengan menggunakan kerangka kerja berbasis risiko dan berfokus pada hasil.

- Mempersiapkan: Kami melindungi dengan cara terus memperbarui Program Keamanan Informasi, yang mencakup kepatuhan terhadap undang-undang setempat atau khusus negara bagian dan/atau negara asing untuk mengantisipasi dan mengidentifikasi potensi ancaman dengan lebih baik;
- Mencegah: Kami melindungi dengan cara tetap berada di depan melalui penerapan kontrol pencegahan untuk mencegah kehilangan, penyalahgunaan dan penggunaan yang tidak tepat atas informasi rahasia dan berhak milik, serta mengurangi jumlah insiden;
- Mendeteksi: Kami melindungi dengan cara membatasi paparan melalui penerapan kontrol detektif termasuk pemantauan firewall, perlindungan anti-spam dan virus, dan pemantauan lainnya; terus memantau semua rekan tim, aplikasi, data, sistem dan jaringan bank;
- Mengurangi: Kami melindungi dengan cara mengurangi insiden melalui kemampuan respons yang sigap dan terkoordinasi;
- Menanggapi/Memulihkan: Kami melindungi dengan cara meningkatkan postur keamanan melalui kemampuan forensik, investigasi, dan pembelajaran yang kuat saat menangani masalah kepatuhan, pertanyaan peraturan perundangan, tindakan disipliner, atau klaim hukum.

[12] Data geolokasi didefinisikan sebagai data yang diambil dari perangkat pengguna yang menunjukkan lokasi geografis perangkat tersebut, termasuk data GPS atau data tentang koneksi dengan peralatan wifi lokal

情報セキュリティ監視に関する通知

発効日：2025年5月1日

はじめに

従業員の雇用契約または請負人の請負契約に記載されている法人（以下、「**当社**」）は、従業員あるいは請負人であるあなたに対して提供された「従業員および請負人のデータ保護に関する通知」（以下、「**DPN**」）の内容を補充するため、この「情報セキュリティ監視に関する通知」[13]（以下、「**本通知**」）を作成しました。本通知は、当社の電子システムおよび電子端末により送受信、処理、および／または保存されるデータおよびその他の資料[14]（業務上または私的なメッセージ、コミュニケーション、および情報を含むが、これらに限らない）に対する監視について、当社における業務慣行を定めるものです。かかる電子システムおよび電子端末には、ネットワーク、音声、コンピューター、当社支給のモバイル機器、インスタントメッセージング、ウェブアプリケーション、モバイルアプリケーション、ソーシャルメディア、音声会議、テレビ会議およびファックスのインフラストラクチャー（以下「**電子コミュニケーション**」）、プリンターの使用、インターネットおよび物理的アクセスログを含みますがこれに限定しません。

本通知は、業務上の目的または監督機能のために当社のシステム、施設および／または情報にアクセスできるすべての個人およびグループに適用され、具体的には、当社の従業員、コンサルタント、請負人、非業務執行取締役、および当社におけるその他の雇用者（各々、「**承認済みユーザー**」）が含まれます。付録Aには、当社が監視し、承認済みユーザーに関する個人を特定可能な情報（「**個人データ**」）を収集することがある通信および記録の非包括的なリスト、および当社が個人情報を使用、移転および開示する目的が記載されています。

提供された言語以外の言語で本通知を必要とする承認済みユーザーは、問合せ先詳細セクションに記載した情報を使用して、グローバル情報セキュリティ部門に問い合わせてください。本通知が英語以外の言語で承認済みユーザーに提供される場合、それら2か国語版の間に不一致、対立または矛盾があれば、当該のDPNにおける規定に基づき解決するものとします。

場所に関係なく、監視ツールおよびプロセスは、現地の法令で禁じられていない範囲で、当社の電子システムおよびデバイスに対して当社が定期的に配置します。当社の電子システムおよびデバイス上で行われる監視活動はすべて、本通知に従って実施されます。

監視プロセスの一環として（直接的または間接的に）収集される個人データは、臨時発行される当該のDPNに基づいて取り扱われるものとします。個人データの処理は、手動ツールおよび電子ツールの助

---

[13]本情報セキュリティ監視に関する通知（ISMN）は、過去において「サイバーセキュリティ監視に関する通知」（CSMN）と題されていたため、当社の他の文書においてはその題名で言及されている場合があります。

[14]行動規範に則して、承認済みユーザーは、個人的な連絡のために、当社の管理下にある機器およびアプリケーションを限定的に個人使用することが許可されています。システムの完全性を保ち、当社に賠償責任やリスクが生じうる行為を回避するために、リソースの使用は監視および調査される場合があります（マルウェアの導入や不適切なデータ送受信に係る監視など）。

けを得て実行されます。

本通知は、関連する当社の方針の重要な部分に言及していますが、電子コミュニケーションとインターネットの使用に適用されるすべての当社の方針および要件を含むものではありません。承認済みユーザーは、当社の行動規範、電子コミュニケーションガイドおよびグローバル情報セキュリティ方針文書、ならびに当社が随時発行するその他の該当する基準に記載された要件を遵守する必要があります。本通知で定義されずに使用される、大文字で記されたすべての用語には、当社のグローバル情報セキュリティ方針文書で定められた意味が適用されるものとします。

規制対象となる特定の当社の社員によるコミュニケーションには、さらに詳細な監督要件が適用されます。承認済みユーザーは、自分の事業部門に関連する方針および手順を参照して、詳細な情報を入手するようにしてください。

適用される法律に従い、当社のコンピューターまたはネットワークのリソースを使用した電子メール（暗号化の有無[15]に関わらず）およびインターネットとイントラネットのウェブサイトへの接続を含むすべての電子コミュニケーションは、当社の財産であり、監視および監査の対象となることがあります。これには、以下が含まれますが、これらに限定されるわけではありません。

- **事前通告を付与せずに監視活動を行うことが許可される場合において、事前通告なしの監視活動（以下、「内密の監視」）を実施する（例：データの不正転送の疑いがある場合、犯罪またはその他の違法な行為が発生した場合、当社のコンプライアンス方針またはグローバル情報セキュリティ方針に違反する行為が発生した場合、または当社に対するその他の責任に違反した行為が発生した場合）、 あるいは当該の法律により、適切な令状や許可に基づき要求される場合。**
- **個人的または内密その他個人的性質のものであることを示す表示のある外部との電子メールその他のメッセージで、電子メールおよびその内容または添付書類が、適用法または当社のコンプライアンスもしくはグローバル情報セキュリティ方針その他の当社が負うべき義務と矛盾する、またはこれに違反する疑いがある場合、かかる電子メールおよびその他のメッセージを監視またはブロックする。**

個人情報の収集と使用目的

当社の電子システムおよびデバイスの特定の監視活動は、本通知の付録Aに記載された目的のために、当社全体で実施されます。

当社が本通知で略述する監視の実施中に処理することがある個人情報のカテゴリーおよび当該処理の法的根拠（必要に応じて、同意を含む）は、関連するDPNに記載されているとおりです。

承認済みユーザーは、追加の権利を持つ場合があります。適用される法律に基づく個人の権利については、当該のDPNに記載されています。（セクションVII：個人データのアクセス、可搬性、修正および抑

[15]暗号化された電子コミュニケーションに対する監視および監査が、暗号の解読および再暗号化を含む場合。

制、処理の制限と限定、および正確性）。

当社は、適用される法律に従って、またさらなる通知なしに、特定の状況下で（特権の昇格、アクセス権の昇格、離職間近などが含まれるが、これらに限定されない）、銀行が提供するコンピューターおよび／またはモバイルデバイスに対するデータ監視機能の強化を導入する権利を留保します。

機密性の高い個人情報

当社は、本通知に記載された活動を実施する過程で、関連するDPNに記載されている機密性の高い個人情報を含む、一定の特別なカテゴリーの個人情報を収集し処理を行うことがあります。

グローバル情報セキュリティの監視活動は、機密性の高い個人データを積極的に監視することはしませんが、一部の機密性の高い個人データは、その他のタイプのデータの監視過程で開示されることが避けられない場合があります。

当社関係者によるアクセス

本通知に従って処理される個人データへのアクセスは、関連するDPNに記載されている目的で、そのようなアクセスを必要とする個人に限定されます。これには、グローバル情報セキュリティチームのメンバー、および承認済みユーザーの本国管轄区域や、当社が事業を展開しているその他の管轄区域における内部企業調査のメンバーが含まれますが、これらに限定されません。

開示

本通知に記載した監視ツールおよびプロセスは、米国、英国、シンガポール、香港、およびインド、ならびに特定の営業国／地域内に所在する当社グローバル情報セキュリティチームが導入する場合があります。個人データは、承認済みユーザーの本国の管轄区域、および／または当社が事業を展開しているその他の管轄区域で保管および／または処理される場合があります。

当社の活動の世界的な性質を鑑みて、当社は、関連するDPNに記載されているとおり、あなたの個人情報をあなたの自国外にある国に移転する場合があります。

当社は、適用法に従って、関連個人情報を関連会社および支店に開示することができ、開示された者は、本通知に記載される目的のために、当該個人情報を処理することができます。さらに、当社は、適用される法律に従って、当該個人情報を、関連するDPNに記載されている特定の第三者に開示することができます。

セキュリティ

個人情報が無断で、または違法に処理されることから保護し、また、偶発的な損失、改変、開示またはアクセス、偶発的あるいは違法な破壊または損害から個人データを保護するため、当社は技術面や組織面で適切な対策を維持しています。

処理の様式とデータ保持

すべての監視、監査活動は、当初個別化されない状態で開始され、本通知に記載した目的において不正使用や異常な行動の徴候が認められた場合のみ、特定の承認済みユーザーをターゲットとして実行されます。個人的に銀行システムを利用した結果、レビューが必要となる個人的なコミュニケーションが発生した場合、かかるレビューは常に適用される法律、規則、および規制に基づいて実行されます。

当社は、本通知に記載した目的のために個人データを処理するにあたり、当該の承認済みユーザーに対して法的または類似の重大な影響を及ぼす決定である場合、本通知に記載されたとおり監視を実施する際に、承認済みユーザーを対象とするプロセスにおいて「自動意思決定」を用いません。「自動意思決定」とは、人による関与なしに、自動的な手段で意思決定を行うプロセスのことです。

各データの種類および法域における保持期間は、Flagscape上のグローバル記録管理に関するページにおける「グローバル記録保持スケジュール」に記載されています。保持要件は、社内サイトにまだアクセスできない新規の承認済みユーザーでも要求に応じて入手することができます。当社は、適用される保持期間が経過した後で、個人データを削除します。

懲戒処分

本通知で言及されている方針のいずれかに違反した承認済みユーザーは、調査、アクセス停止、および／または懲戒措置（最大で解雇または契約業務の終了を含む）の対象となることがあります。従業員ではない承認済みユーザーは、自身の雇用主による懲戒処分の対象となることがあります。適用される法律または規制に違反した承認済みユーザーは、法規制上の要件に従い、法執行機関および／または規制当局に報告されます。電話、電子メール、インターネットまたはイントラネットの使用（個人的な電話、電子メールおよびインターネットの使用を含む）の監視を通して確認されたデータまたは証拠（上記の例が含まれるが、これらに限定されない）は、懲戒措置および内部調査または外部調査において、証拠として使用されることがあります。承認済みユーザーは、要請された場合、質問、検査、活動の監視および記録に協力することが求められます。セキュリティに関する調査への協力を拒否すると、解雇または契約業務の解約を含む、法的または懲戒処分の対象となることがあります。

連絡先の詳細

承認済みユーザーが本通知またはグローバル情報セキュリティ監視活動に関して質問したい場合や詳細情報が必要な場合は、グローバル情報セキュリティ.

あなたは、自国のデータ保護当局に苦情を申し立てる権利を有する場合があります。権利の適用性と詳細情報については、関連するDPNを参照してください。

現地の法規制に関する質問がある場合、承認済みユーザーは、現地のコンプライアンス担当オフィサー、データ保護オフィサー、または法務部に問い合わせてください。

本通知の変更

本通知は契約ではなく、当社は、本通知をいつでも修正または撤回する権利を留保します。当社が本通知について大幅な変更を行う場合、当社は改訂通知の再発行および／または適用法に従ってその他の措置を講じることにより、可能な限り合理的に速やかに、承認済みユーザーに通知します。

付録A

以下に要約される各使用目的のために収集される可能性のあるデータの種類を閲覧するには、こちらのリンク先のマトリックスをご参照ください。このマトリックスは、社内サイトにまだアクセスできない新規の承認済みユーザーでも要求に応じて入手することができます。

当社の電子システムおよびデバイス上で当社が監視し、個人データを収集することがあるコミュニケーションおよび記録（その場で、および事後の両方）は、以下を含みますがこれに限定されません。

- 送信済電子メール
- 受領済電子メール
- ウェブ／インターネットの使用、FTP、HTTP、HTTPS、テルネット
- 印刷の履歴および内容
- デスクトップ（My Documentsフォルダは除く）、コラボレーションサイト、オープンシェア、または社内Wiki上で保存されたファイル
- リムーバブルメディア、当社システムに接続できる当社管理外の端末
- インスタントメッセージ
- 電話による通話、VoIP による通話、ボイスメール
- アプリケーションアクセスならびに使用ログおよび記録
- ネットワークアクセス情報（IPアドレスおよびISPを含む）
- システムアクセスならびに使用ログおよび記録（使用および行動の経過を示す記録を含む）
- ファックスおよびドキュメント・スキャニング／イメージング
- ソーシャルメディアの使用および内容（外部、当社以外）
- オープンソースおよび公有情報
- セキュリティログ
- キーログおよびスクリーンショット
- ビデオ会議関連のテクノロジー
- クッキー、ビーコン、シンクホール、ハニーポット
- 位置情報データ[16]
- スワイプカードの入力データ
- 送受信したテキストメッセージ

当社が個人情報を収集、使用、移転および開示する目的:

グローバル情報セキュリティ方針は、常に変化を続ける情報セキュリティに対する脅威に対して、当社が準備、防止、検知、対応、および復旧するために必要な要件を定めることを目的とするものです。グローバル情報セキュリティプログラムは、情報セキュリティ上の脅威によるお客様からの信頼低下や業務の中断を防止するために、高度な防御テクニックを用いたソリューションを提供するものです。グローバル情報セキュリティは、リスクベースかつ成果重視のフレームワークに基づき、当社およびお客様を

[16] 位置情報データとは、GPSデータや現地Wi-Fi機器への接続に関するデータなど、ユーザーのデバイスから取得されたデータで、そのデバイスの地理的位置を示すものと定義されます。

保護します。

- 準備：当社では、継続的に情報セキュリティプログラムを更新して保護を実現します。これには、潜在的な脅威を予測し、特定する能力を高めるために、現地または海外の政府及び／又は国家が定めた特定の法律を遵守することが含まれます。
- 防止：当社は、機密情報および独占情報の損失、不正使用、または不適切な使用を防止し、インシデントの件数を削減するために必要な予防的統制を導入し、攻撃者の先手を取ることで保護を実現します。
- 検知：当社は、ファイアーウォールの監視、スパムおよびウイルス対策、およびその他の監視機能を含む検知関連の統制を導入すると共に、当社におけるすべての従業員、アプリケーション、データ、システム、およびネットワークに対する継続的な監視を通じて、脅威へのエクスポージャーを軽減して保護を実現します。
- 軽減：当社は、迅速かつ連携が取れた対応能力を通じて、インシデントの深刻さを引き下げることで保護を実現します。
- 対応／復旧：当社は、コンプライアンス関連の問題や規制当局からの問い合わせ、懲戒処分、または法的な申立に対応しつつ、フォレンジック、調査、および過去の事例に基づく充実した対応能力を通じてセキュリティ姿勢を強化し、保護を実現します

정보 보안 모니터링 고지

발효일: 2025년 5월 1일

소개

직원의 고용 계약 또는 협력업체의 계약에 명시된 법인(이하 "**회사**")은 본 정보 보안 모니터링 고지[17](이하 "**고지**")를 작성하여 회사의 전자 시스템 및 기기에 의해 전송, 수신, 처리 및/또는 저장된 데이터 및 기타 자료(업무 및 개인 메시지, 통신 및 정보를 포함하되 이에 국한되지 않음)의 모니터링에 관한 관행을 설명하기 위해 직원 또는 협력업체로서 귀하가 받는 직원 및 협력업체 데이터보호 고지(이하 "DPN")를 보완합니다.[18] 여기에는 네트워크, 음성, 컴퓨터, 회사가 제공한 휴대 기기, 인스턴트 메시지, 웹 애플리케이션, 모바일 앱, 소셜 미디어, 오디오 컨퍼런스, 동영상 컨퍼런스, 팩스 인프라("**전자 커뮤니케이션**"), 프린터 사용, 인터넷 및 물리적 접속 기록이 포함되나 이에 국한되지 않습니다.

본 고지는 회사의 직원, 컨설턴트, 협력업체, 비상임 이사 및 기타 근로자를 포함하여, 사업상의 목적으로, 또는 감독 업무를 위해 회사의 시스템, 시설 및/또는 정보에의 접근을 제공받은 모든 개인 또는 그룹에 적용됩니다(각각 "**승인된 사용자**"). 부록 A는 당사가 모니터링하고 승인된 사용자에 대해서 개별적으로 식별 가능한 정보(이하 "**개인 데이터**")를 수집할 수 있는 커뮤니케이션 및 기록의 불완전한 목록 및 당사가 개인 데이터를 사용, 이전 및 공개하는 목적을 제시합니다.

제공된 언어 이외의 언어로 본 고지가 필요한 승인된 사용자는 연락처 세부 정보 섹션에 명시된 정보를 사용하여 글로벌 정보 보안 부서에 연락해야 합니다. 이 고지가 영어 이외의 언어로 승인된 사용자에게 제공될 경우, 두 언어 버전 간의 모든 차이, 상충 또는 불일치는 관련 DPN에 명시된 대로 해결되어야 합니다.

위치, 모니터링 도구 및 프로세스에 관계없이 현지의 법률 또는 규정이 금지하지 않는 범위 내에서 회사는 회사의 전자 시스템 및 기기에 통상적으로 이를 적용합니다. 회사의 전자 시스템 및 기기에서 일어나는 모든 모니터링 활동은 본 고지에 따라 수행됩니다.

모니터링 프로세스 과정에서 (직간접적으로) 수집된 일체의 개인 데이터는 수시로 발행되는 관련 DPN에 따라 취급됩니다. 개인 데이터 처리는 수동 및 전자 도구를 이용하여 수행합니다.

본 고지는 관련된 회사 정책의 핵심 부분을 언급하지만, 전자 커뮤니케이션 및 인터넷 사용에 적용되는 회사의 모든 정책 및 요건을 포함하지는 않습니다. 승인된 사용자는 회사의 행동 강령, 전자 커뮤니케이션 가이드 및 글로벌 정보 보안 정책 문서에 명시된 요건뿐 아니라 회사가 수시로

---

[17] 정보 보안 모니터링 고지(ISMN)는 이전에는 사이버 보안 모니터링 고지(CSMN)라고 불렸으며 다른 회사 문서에서는 그렇게 칭할 수도 있습니다

[18] 행동 강령에 따라, 승인된 사용자는 회사가 관리하는 기기 및 개인 커뮤니케이션을 위한 앱, 인터넷 및 이메일의 제한적인 사용이 허용됩니다. 시스템의 무결성을 유지하고(예: 악성 소프트웨어 침입 또는 부적절한 데이터 전송의 모니터링) 회사에 법적 책임 또는 위험을 야기시킬 수 있는 활동을 피하기 위해서 자원의 사용이 모니터링되고 검사될 수 있습니다.

발표하는 일체의 기타 해당 표준을 준수해야 합니다. 본 고지에서 사용되었지만 정의되지 않은 모든 대문자로 시작하는 용어는 회사의 글로벌 정보 보안 정책 문서에서 의미가 배정됩니다.

특정 통제를 받는 회사 직원에 의한 커뮤니케이션은 추가적인 세부 감독 요건의 대상이 되며, 승인된 사용자가 추가 정보를 얻으려면 사업 분야에 대한 관련 정책 및 절차를 참고해야 합니다.

해당 법률에 따라 이메일(암호화된[19] 이메일 및 암호화되지 않은 이메일) 및 회사의 컴퓨팅 또는 네트워크 자원을 이용하는 인터넷 및 인트라넷 웹사이트에의 접속을 비롯한 모든 전자 커뮤니케이션은 회사의 재산이며 모니터링 및 감시의 대상이 될 수 있습니다. 여기에는 다음이 포함되나 이에 국한되지 않습니다.

- **허용된 경우(예: 데이터 유출, 범죄 또는 기타 위법 활동 또는 회사의 준법 또는 글로벌 정보 보안 정책의 위반 또는 회사에 대한 기타 의무 사항의 위반 등이 의심되는 경우) 또는 해당 법률에 의해 요구되거나 관련 영장이나 승인에 근거하여 사전 고지 없이 모니터링 활동을 수행할 수 있습니다.**
- **개인적이거나 사적 또는 달리 개인적인 성격의 것임을 나타내는 수신 및 발신 이메일과 기타 메시지를 모니터링하고/모니터링하거나 차단할 수 있습니다. (그러한 이메일 및 그 내용이나 첨부 파일이 해당 법률이나 회사의 준법 또는 글로벌 정보 보안 정책 또는 회사에 대한 일체의 기타 의무 사항을 위배 또는 위반한다는 의심이 있는 경우).**

개인 데이터 수집 및 사용 목적

회사의 전자 시스템 및 기기에 대한 특정 모니터링 활동은 본 고지의 부록 A에 제시된 목적을 위해 회사 전체에 걸쳐 실시됩니다.

본 고지에 약술된 모니터링의 착수 과정에서 회사가 처리할 수 있는 개인 데이터의 범주 및 그러한 처리에 대한 법적 근거(필요한 경우, 동의 포함)는 관련 DPN에 제시된 바와 같습니다.

승인된 사용자는 추가 권리를 가질 수 있습니다. 해당 법률에 따라 개인의 권리는 관련 DPN에 명시되어 있습니다. (섹션 VII: 개인 데이터의 접근, 이동, 수정 및 억제, 처리의 제한 및 제약, 정확성).

회사는 관련 법률에 따라 추가 고지 없이 특정 상황(높은 권한, 높은 액세스 권한 또는 다가오는 출발 날짜를 포함하되 이에 국한되지 않음)에서 은행이 제공한 컴퓨터 및/또는 모바일 기기에 강화된 데이터 모니터링을 배포할 권리를 보유합니다.

민감한 개인 데이터

회사는 관련 DPN에 제시된 바와 같이 본 고지에서 설명하는 활동들의 수행 과정에서 민감한 개인 데이터를 비롯한 개인 데이터의 특정 특수 범주를 수집 및 처리할 수 있습니다.

글로벌 정보 보안 모니터링 활동에서는 민감한 개인 데이터를 적극적으로 모니터링하지는 않지만

19 암호화된 커뮤니케이션의 모니터링 및 감시가 암호화의 차단 및 재적용과 관련된 경우.

일부 민감한 개인 데이터는 기타 유형의 데이터를 모니터링하는 동안 불가피하게 공개될 수 있습니다.

회사 직원에 의한 접근

본 고지에 따라 처리된 개인 데이터에 대한 접근은 관련 DPN에 명시된 목적을 위해 그러한 접근이 필요한 개인으로 제한되며, 여기에는 승인을 받은 사용자의 거주국 관할권 및/또는 회사가 사업을 운영하는 기타 관할권에서의 글로벌 정보 보안팀 및 내부 기업 조사팀의 구성원이 포함되나 이에 국한되지 않습니다.

공개

본 고지에서 설명하는 모니터링 도구 및 프로세스는 미국, 영국, 싱가포르, 홍콩 및 인도에 소재한, 그리고 사업이 운영되는 특정 국가/지역 내의 회사 및 회사의 모든 계열사 및 지점의 글로벌 정보 보안팀이 활용할 수 있습니다. 개인 데이터는 승인된 사용자의 거주국 관할권 및/또는 회사가 사업을 운영하는 다른 관할권에서 저장 및/또는 처리할 수 있습니다.

전 세계적으로 이루어지는 회사 활동의 특성상 회사는 관련 DPN에 제시된 바와 같이 사용자의 개인 데이터를 본국 이외의 국가로 이전할 수 있습니다.

회사는 해당 법률에 따라 그 계열사 및 지점 일체에 관련 개인 데이터를 공개할 수 있으며 이들 계열사 및 지점들은 본 고지에 제시된 목적을 위해 그러한 개인 데이터를 처리할 수 있습니다. 또한 회사는 해당 법률에 따라 관련 개인 데이터를 관련 DPN에 정한 바와 같은 특정 제3자에게 공개할 수 있습니다.

보안

회사는 무단 또는 불법적인 개인 데이터 처리 및/또는 개인 데이터에 대한 우발적인 분실, 변경, 공개, 접근 또는 우발적 또는 불법적 파괴나 훼손으로부터 보호하기 위한 적절한 기술적 및 조직적 조치를 유지해야 합니다.

처리 방법 및 데이터 보관

모든 모니터링 및 감시 활동은 처음에는 특정 개인을 대상으로 하지 않으며, 본 고지에 명시된 목적을 위해 남용 또는 불규칙한 행동의 징후가 있는 경우에만 승인된 특정 사용자를 대상으로 합니다. 은행 시스템을 개인적으로 사용하여 검토가 필요한 개인 커뮤니케이션이 이루어지는 경우, 해당 법률, 규칙 및 규정에 따라 검토를 수행합니다.

본 고지에 명시된 목적을 위해 개인 데이터를 처리함에 있어, 회사는 본 고지에 기술된 대로 모니터링을 수행할 때 의사 결정이 승인된 사용자에게 법적 영향 또는 이와 비슷하게 중요한 영향을 끼치는 경우 승인된 사용자 프로세스에 대해 자동 의사 결정을 사용하지 않습니다. '자동 의사 결정'은 인간이 개입하지 않은 자동화 수단에 의한 의사 결정 프로세스입니다.

각 데이터의 유형 및 관할권에 대한 보관 기간 정보는 Flagscape 글로벌 기록 관리 페이지의 글로벌

기록 보관표에 설명되어 있습니다. 아직 내부 사이트에 접속 권한이 없는 새로 승인된 사용자의 경우 요청 시 보관 요건을 확인할 수 있습니다. 회사는 해당 보관 기간이 경과한 개인 데이터를 삭제할 것입니다.

징계 조치

본 고지에 명시된 일체의 정책을 위반하는 승인된 사용자는 조사, 접근 정지 및/또는 징계 절차(최대 고용 또는 계약 서비스 종료 포함)를 받을 수 있습니다. 직원이 아닌 승인된 사용자는 징계 조치를 위해 소속 고용주에게 통지될 수 있습니다. 해당 법률 또는 규정을 위반한 승인된 사용자는 법률 및 규정 요건에 따라 사법 및/또는 규제 기관의 담당자에게 통지될 수 있습니다. 전화 통화, 이메일 및 인터넷이나 인트라넷 사용(개인적인 전화 통화, 이메일 및 인터넷 사용 포함)의 모니터링(이를 포함하지만 이에 국한되지는 않음)을 통해 식별된 모든 자료 또는 증거는 일체의 징계 조치 및 내부 또는 외부 조사 과정에서 사용될 수 있습니다. 승인된 사용자는 요구되는 경우, 조회, 검사, 모니터링 및 기록 활동에 협조해야 합니다. 보안 조사에 협조를 거부하는 경우 고용 또는 계약 서비스의 종료를 포함하여, 법적 또는 징계적 조치를 야기할 수 있습니다.

연락처 세부 정보

이 공지 또는 글로벌 정보 보안 모니터링 활동에 대한 질문 이나 자세한 내용은 권한이 있는 사용자는 글로벌 정보 보안에 문의해야 합니다.

귀하는 거주 중인 국가의 데이터 보호 당국에 불만을 제기할 권리가 있습니다, 적용 가능성 및 추가 정보는 관련 DPN을 참조해 주십시오.

현지 법률 및 제약에 관한 질문을 하려면, 승인된 사용자는 현지 규정준수 책임자, 데이터 보호 책임자 또는 법무부서에 문의해야 합니다.

이 고지의 변경 사항

본 고지는 계약에 의한 내용이 아니며, 회사는 언제든 필요한 경우 본 고지를 수정하거나 철회할 권한을 갖습니다. 회사가 본 고지에 대해 상당한 수정을 가할 경우, 회사는 수정된 고지를 재발표하고/하거나 해당 법률에 따라 기타 조치를 취함으로써 합리적으로 가능한 한 빨리 승인된 사용자에게 통지할 것입니다.

부록 A

아래에 요약된 각 사용 목적에 따라 수집될 수 있는 데이터의 범주를 확인하려면 여기에 링크된 매트릭스를 참조하시기 바랍니다. 아직 내부 사이트에 접속 권한이 없는 새로 승인된 사용자의 경우 요청 시 매트릭스를 확인할 수 있습니다.

회사가 회사의 전자 시스템 및 기기에서 모니터링하고 개인 데이터를 수집할 수 있는 커뮤니케이션 목록 및 기록(현재 발생 중인 경우 및 발생한 이후의 경우 모두)에는 다음이 포함되나 이에 국한되지 않습니다.

- 보낸 이메일
- 받은 이메일
- 웹 / 인터넷 사용, FTP, HTTP, HTTPS, 텔넷
- 인쇄 사용 및 내용
- 데스크탑에 보관된 파일(My Documents 외부), 협업 사이트, 공개 공유, 사내 Wiki's
- 리무버블 미디어, 회사 시스템에 연결되는 비회사 관리 기기
- 인스턴트 메시징
- 전화 통화, VOIP 통화, 음성사서함
- 애플리케이션 액세스 및 사용내역 로그와 기록
- 네트워크 접속 정보(IP 주소 및 ISP 포함)
- 시스템 액세스 및 사용내역 로그와 기록(사용 및 수행 과정을 보여주는 기록 포함)
- 팩스 및 문서 스캐닝/이미징
- 소셜 미디어 사용 및 내용(외부, 비회사)
- 오픈 소스 및 공개적으로 이용 가능한 정보
- 보안 로그
- 키로그 및 스크린샷
- 컨퍼런싱 기술
- 쿠키, 비콘, 싱크홀 및 허니팟
- 지리적 위치 데이터[20]
- 전자 카드 출입 데이터
- 보내고 받은 문자 메시지.

회사가 개인 데이터를 수집, 사용, 이전 및 공개할 수 있는 목적:

글로벌 정보 보안 정책은 회사가 증가하는 위협 환경의 변화를 대비, 방지, 탐지, 대응 및 복구할 수 있도록 필요한 요구사항을 제공하도록 설계되었습니다. 글로벌 정보 보안 프로그램은 솔루션을 제공하고 고급 기술을 사용하여 정보 보안 위협으로 인해 고객의 신뢰를 훼손하고 비즈니스 운영이 중단되는 것을 방지합니다. 글로벌 정보 보안은 위험 기반 및 결과 중심 프레임워크를 사용하여 회사와 고객을 보호합니다.

- 대비: 회사는 잠재적 위협을 더 잘 예측하고 식별하기 위해 현지 또는 외국 및/또는 국가별 법률을 준수하는 것을 포함하는 정보 보안 프로그램을 지속적으로 업데이트하여 보호합니다.
- 예방: 기밀 정보 및 독점 정보의 손실, 오용 및 부적절한 사용을 방지하고 사고 발생 수를 줄이기 위한 예방적 통제를 구축하여 적보다 앞서서 보호합니다.
- 탐지: 회사는 방화벽 모니터링, 스팸 방지 및 바이러스로부터의 보호, 기타 모니터링을 포함한 탐지 제어장치 배치를 통해 노출을 제한하여 보호하며, 모든 은행 팀원, 애플리케이션, 데이터, 시스템 및 네트워크를 지속적으로 모니터링합니다.

[20] 지리적 위치 데이터는 GPS 데이터 또는 로컬 와이파이 장비와의 연결에 대한 데이터를 포함하여 해당 장치의 지리적 위치를 나타내는 사용자의 장치에서 가져온 데이터로 정의됩니다.

- 완화: 회사는 민첩하고 조정된 대응 기능을 통해 사고를 완화하여 보호합니다.
- 대응/복구: 회사는 규정 준수 문제, 규제 문의, 징계 조치 또는 법적 청구를 처리하는 동안 강력한 포렌식, 조사 및 학습된 기능을 통해 보안 태세를 개선하여 보호합니다.

資訊安全監控公告

生效日期：2025 年 5 月 1 日

引言

員工的僱傭契約或承包商的委任書中所載明之法律個體（下稱「**本公司**」）制訂了本資訊安全監控公告[21]（下稱「**本公告**」），以針對您身為員工或承包商所收受的員工和承包商資料保護須知（下稱「**DPN**」）進行內容補充，以就本公司電子系統與裝置所傳輸、收受、處理及/或儲存的資料及其他材料（包括但不限於：業務與私人[22]訊息、通訊及資訊）的監控作業，訂立相關實務做法。這些電子系統及裝置包括但不限於網路、語音、電腦、公司核發之行動裝置、即時通訊、網路應用程式、社群媒體、音訊會議、視訊會議和傳真基礎設施（下稱「**電子通訊**」）、印表機的使用、網際網路及實體存取紀錄檔。

本公告適用於已基於業務目的或監督職能獲得存取本公司系統、設施及/或資訊權限之所有個人或團體，包括本公司的員工、顧問、承包商、非執行董事、及其他工作人員（各稱為「**授權使用者**」）。附錄 A 載明了我們所監控的通訊及紀錄的非完整清單，而且我們得在監控時蒐集授權使用者的任何個人可識別資訊（下稱「**個人資料**」），附錄 A 亦載明了我們得使用、傳輸及揭露個人資訊的目的。

授權使用者如要求以我們所提供語言版本以外之其他語言取得本公告者，應利用聯絡資訊部分所載資訊聯絡全球資訊安全部門。本公告以英文外的語言向授權使用者提供時，兩種語言版本間如有任何差異、相互牴觸或不一致之處者，應按照相關 DPN 規定予以解決。

不管地點在哪裡，本公司都會在當地法律或規範未禁止範圍內，對本公司的電子系統與裝置部署例行監控工具與流程。對本公司的電子系統與裝置進行的一切監控活動，均依照本公告規定辦理。

監控流程期間所（直接或間接）蒐集之任何個人資料，應依據不定時發佈之相關 DPN 規定予以處理。個人資料處理會在人工和電子工具的協助下進行。

本公告參考本公司相關政策的主要部分，但並未涵蓋本公司所有適用於電子通訊及網際網路使用情形的政策及要求。授權使用者必須遵守在本公司行為準則、電子通訊指南及全球資訊安全政策文件以及本公司不定時發佈之其他任何適用標準所載明之規定。在本公告中使用但未定義的所有大寫術語，均擁有本公司全球資訊安全政策文件中所定義之涵義。

---

[21] 資訊安全監控公告（ISMN）的原始標題為網路安全監控公告（CSMN），並且在公司其他文件中亦得使用該標題指稱資訊安全監控公告。

[22] 為符合行為準則規定，授權使用者僅得基於個人通訊目的，對公司管理裝置與應用程式、網際網路及電子郵件做有限度的私人使用。對於資源的使用情形，可能會受到監控及查核，以維持系統完整性（例如：監控任何導入惡意程式或不當資料傳輸情事），並避免可能導致公司遭受法律責任或風險的活動。

特定本公司受規範人員之通訊，係受額外詳細監管要求之規範限制，授權使用者務必就其業務範圍參考相關政策及程序，以獲取進一步資訊。

在符合相關法律規範情況下，所有電子通訊（包括電子郵件（加密[23]與未加密））以及透過本公司運算或網路資源與網際網路及內部網路網站之連線，均屬於本公司的財產，並且可能受到監控與監視。其中包括但不限於：

- **在受到許可的情況下（例如，強烈懷疑存在資料外滲、犯罪或其他非法活動、或違反本公司法令遵循或全球資訊安全政策、或違反應對本公司承擔之其他任何義務的行為），或在相關法律有所規定並取得相關法院令狀或授權情況下，未發事先通知即執行監控活動（下稱「秘密監控」）；**
- **如其懷疑該等電子郵件及其內容或附件違反適用法律、本公司法令遵循或全球資訊安全政策，或違反應對本公司承擔之其他任何義務者，得監控及/或封鎖寄入及寄出之電子郵件及其他標記為個人或私密或其他具私人性質的訊息傳送情形。**

個人資料蒐集及使用目的

本公司已基於本公告附錄 A 所載目的，在本公司整體上下對本公司的電子系統與裝置實行若干監控活動。

本公司在進行本公告所述之監控作業時，可能處理之個人資料類別，及該等資料處理作業之法律基礎（視必要情況亦包括同意），均載於相關 DPN 中。

授權使用者可能擁有額外權利。在符合相關法律限制下，個人的權利已載明於相關 DPN 中。（第七節：個人資料的存取、可攜性、訂正與隱匿、限縮與限制處理及準確性）。

本公司保留在特定情況下（包括但不限於您擁有提升權限、提升存取權限或即將離職）依據適用法律對您銀行提供的電腦和/或行動裝置部署強化資料監控之權利，恕不另行通知。

敏感性個人資料

本公司在執行本公告所述活動期間，得蒐集及處理相關 DPN 所訂之若干特殊類別之個人資料，其中包括敏感性個人資料。

全球資訊安全監控活動並不會對敏感性個人資料進行主動監控，但在監控其他類別的資料期間，可能會無可避免地揭露部分敏感性個人資料。

公司工作人員之存取權限

依據本通知所處理之個人資料的存取權限，僅限於為相關 DPN 所列目的而需要此類存取權限之人員，包括但不限於全球資訊安全團隊成員及內部企業調查人員，無論其位於授權使用者的所在地

23對加密通訊的監控與監視涉及對加密的破解與重新套用。

管轄區域及 / 或公司營運之其他管轄區域。

揭露

本公告所述之監控工具與流程，得由本公司及其任何關係企業與分公司的全球資訊安全團隊進行部署，其中包括位於美國、英國、新加坡、香港和印度、及營運所在特定國家/地區的關係企業與分公司。個人資料可能在授權使用者的所在國司法轄區及/或本公司經營業務所在的其他司法管轄區保存及/或處理。

鑒於本公司業務活動遍及全球，因此本公司得按照相關 DPN 規定，把您的個人資料傳輸至您所在國以外之國家。

本公司得根據適用法律，向其任何關係企業和分公司揭露相關個人資料，且該等關係企業及分公司得基於本公告所載目的，處理該等個人資料。此外，本公司得依據適用法律，向相關 DPN 所載特定第三方，揭露相關個人資料。

安全性

本公司維持適當的技術性與組織性措施，以防範未經授權或非法的個人資料處理情事、及/或意外遺失、竄改、揭露或存取情事，或意外或非法銷毀或破壞個人資料情事。

處理和資料保留的方式

基於本公告所訂目的，所有監控與監視活動在一開始都不會針對任何個人，只有在出現濫用或異常行為的跡象時，才會針對特定授權使用者進行。如有對銀行系統的私人使用情形，導致需要對私人通訊進行審查者，任何審查作業都會依據相關法律、規則、規範辦理。

在基於本公告所載目的處理個人資料時，如果在按本公告所述方式進行監控作業時所做的決定會對授權使用者產生法律效力或類似重大效力時，本公司不會對授權使用者流程使用自動化決策機制。「自動化決策機制」係指以自動化工具做決策的程序，並且無任何人類的參與。

各類別資料與各司法轄區的保留期間，均載明於全球記錄保留時間表，該時間表可以在 Flagscape 上的全球記錄管理頁面查閱。新進但尚未獲得內部網站存取權限之授權使用者，在提出要求後亦可查閱資料保留相關規定。本公司將在適用保留期過後刪除個人資料。

紀律處分

違反本公告提及的任何政策的獲授權使用者可能要接受調查、被中止存取權和/或按紀律程序進行處理（嚴重者包括終止僱傭或承包服務）。非屬員工的授權使用者可能會交由其僱主進行紀律處分。違反適用法律或規範的授權使用者，可能會根據法律及監管要求交由執法及 / 或監管官員處理。在任何紀律程序及內部或外部調查中，可能倚靠透過（包括但不限於）電話監控、電子郵件及網際網路或內部網路使用（包括個人電話、電子郵件及網際網路使用）發現的任何材料或證據。我們期望獲授權使用者在被要求時配合質詢、檢查、監控及記錄活動。拒絕配合安全調查可能導致法律或紀律處分，包括終止僱傭或承包服務。

聯絡資訊

有關本聲明或全球資訊安全監控活動的問題或更多資訊，授權使用者應聯繫全球資訊安全。

您可能有權利向您所在國家的資料保護主管機關提出申訴，相關適用情形及進一步資訊，請參閱相關 DPN。

關於當地法律及限制的問題，授權使用者應聯絡其當地合規官、資料保護官或法律部。

對本公告之修訂

本公告不具契約性質，且本公司保留隨時修改或撤銷本公告之權利。若本公司對本公告進行重大變更，將根據相關法律，重新發佈經修訂公告及/或採取其他步驟，以便在合理情況下儘快通知授權使用者。

附錄 A

請參閱這裡所連結的矩陣，查看針對各種用途可能蒐集的資料類別，其摘要如後所述。新進且尚未獲得內部網站存取權限之授權使用者，在提出要求後，亦可查看該矩陣。

我們在本公司的電子系統與裝置上監控及可能用以蒐集個人資料之通訊和紀錄（包括現場及事後）包括但不限於：

- 已寄出的電子郵件；
- 已收到的電子郵件；
- Web/網際網路使用、FTP、HTTP、HTTPS、Telnet；
- 列印使用情形與內容；
- 位於桌面（「我的文件」以外）、共同合作站點、open shares、內部 Wiki 上的檔案；
- 連接至本公司系統的卸除式媒體、非公司管理裝置；
- 即時訊息；
- 電話通話、VOIP 通話、語音郵件；
- 應用程式存取和使用記錄檔與記錄；
- 網路存取資訊（包括 IP 位址和 ISP）；
- 系統存取和使用記錄檔與記錄（包括顯示使用和執行過程的記錄）；
- 傳真和文檔掃描/影像；
- 社群媒體的使用情形及內容（外部，非公司）；
- 開源和公開發佈的資訊；
- 安全記錄檔；
- 金鑰紀錄檔及螢幕擷圖；
- 會議技術；
- Cookie、網路信標、坑洞（Sinkhole）及蜜罐（Honeypot）；

- 地理位置資料[24]
- 磁條卡輸入資料；
- 已發送與接收之文字訊息。

我們得蒐集、使用、傳輸和揭露個人資料的目的：

全球資訊安全政策的目的在於訂立必要規定，讓本公司能夠為威脅局勢中愈來愈多的變動做好準備、防範、偵測、應變並從中復原。全球資訊安全計畫提供了解決方案並使用高階技術來防範資訊安全威脅，以免破壞顧客信心及中斷業務營運。全球資訊安全透過基於風險且專注成果的架構，保護本公司及其客戶。

- 準備：我們持續更新資訊安全計畫，進而保護本公司及其客戶，其中包括遵守當地或外國州及/或國家特定法律，以提升我們預期並識別潛在威脅的能力；
- 防範：我們比對手更超前部署預防性控制措施，以避免損失、濫用及不當使用機密與專有資並及減少事故數量，進而保護本公司及其客戶。
- 偵測：我們部署偵測性控制措施，以限制曝險，進而保護本公司及其客戶，包括防火牆監控、反垃圾郵件與病毒防護、及其他監控作業；持續監控所有銀行團隊隊員、應用程式、資料、系統與網路；
- 減緩：我們透過敏捷與協調的應變能力，減緩事故發生，進而保護本公司及其客戶；
- 應變/復原：我們透過穩健的鑑識、調查及經驗學習能力，提升安全性狀態，同時處理任何法令遵循問題、監管詢問、懲處行動或法律請求權主張，進而保護本公司及其客戶。

[24]地理位置資料定義為從使用者裝置取得的資料，指出該裝置的地理位置，包括 GPS 資料或連結當地 wifi 設備的相關資料

NOTIS PEMANTAUAN KESELAMATAN MAKLUMAT

Berkuat kuasa: 1hb Mei 2025

PENGENALAN

Entiti undang-undang yang dinyatakan dalam kontrak pekerjaan Pekerja, atau pelantikan Kontraktor ("**Syarikat**") telah menyediakan Notis Pemantauan Keselamatan Maklumat[25] ("**Notis**") ini sebagai tambahan kepada Notis Perlindungan Data Pekerja dan Kontraktor ("**DPN**") yang anda terima sebagai seorang pekerja atau kontraktor, untuk menetapkan amalan syarikat berkaitan pemantauan data dan bahan lain (termasuk tetapi tidak secara eksklusif, mesej perniagaan dan peribadi[26], komunikasi dan maklumat) yang dihantar, diterima, diproses dan/atau disimpan oleh sistem dan peranti elektronik Syarikat. Ini termasuk, tetapi tidak terhad kepada rangkaian, suara, komputer, peranti mudah alih yang diberikan oleh syarikat, pemesejan segera, aplikasi web, aplikasi mudah alih, media sosial, persidangan audio, persidangan video dan infrastruktur faks ("**Komunikasi Elektronik**"), penggunaan pencetak, Internet, dan log akses secara fizikal.

Notis ini terpakai kepada semua individu atau kumpulan yang telah diberikan akses kepada sistem, kemudahan dan/atau maklumat Syarikat bagi tujuan perniagaan atau fungsi penyeliaan, termasuk pekerja, perunding, kontraktor, pengarah bukan eksekutif dan pekerja-pekerja lain dalam Syarikat (setiap satu "**Pengguna yang Diberi Kebenaran**"). Lampiran A menyediakan satu senarai yang tidak lengkap bagi komunikasi dan rekod yang kami pantau dan yang mungkin kami gunakan untuk mengumpul sebarang maklumat yang boleh mengenal pasti secara individu Pengguna yang Diberi Kebenaran ("**Data Peribadi**") dan tujuan yang mana kami mungkin menggunakan, memindahkan dan mendedahkan Data Peribadi.

Pengguna yang Diberi Kebenaran yang memerlukan Notis ini dalam bahasa selain daripada yang diberikan hendaklah menghubungi Keselamatan Maklumat Global menggunakan maklumat yang ditetapkan dalam bahagian Butiran Hubungan. Sekiranya Notis ini diberikan kepada Pengguna yang Diberi Kebenaran dalam bahasa selain daripada bahasa Inggeris, sebarang percanggahan, konflik atau butiran yang tidak konsisten antara dua versi bahasa ini hendaklah diselesaikan seperti yang ditetapkan dalam DPN yang berkaitan.

Tanpa mengira lokasi, Syarikat menggunakan secara rutin alat dan proses pemantauan dalam sistem dan peranti elektronik Syarikat setakat yang tidak dilarang di bawah undang-undang atau peraturan tempatan. Semua aktiviti pemantauan yang berlaku pada sistem dan peranti elektronik Syarikat dijalankan mengikut Notis ini.

Sebarang Data Peribadi yang dikumpul (secara langsung atau tidak langsung) semasa proses pemantauan

[25] Notis Pemantauan Keselamatan Maklumat (ISMN), sebelum ini digelar Notis Pemantauan Keselamatan Siber (CSMN). Ia juga mungkin dirujuk seperti ini dalam dokumentasi lain syarikat

[26] Selaras dengan Tatakelakuan, Pengguna yang Diberi Kebenaran boleh menggunakan secara terhad, peranti dan aplikasi, internet dan e-mel yang diuruskan oleh syarikat untuk komunikasi peribadi. Penggunaan sumber-sumber ini boleh dipantau dan diperiksa untuk mengekalkan integriti sistem (contohnya, pemantauan untuk perisian hasad atau penghantaran data yang tidak sesuai) dan menghindari aktiviti yang boleh menimbulkan liabiliti atau risiko kepada syarikat.

akan dikendalikan mengikut DPN yang berkaitan seperti yang dikeluarkan dari semasa ke semasa. Pemprosesan Data Peribadi dijalankan dengan bantuan alat manual dan elektronik.

Notis ini merujuk kepada bahagian utama dasar Syarikat yang berkenaan, tetapi tidak mengandungi semua dasar dan keperluan Syarikat yang terpakai bagi penggunaan Komunikasi Elektronik dan Internet. Pengguna yang Diberi Kebenaran dikehendaki mematuhi keperluan yang dinyatakan dalam Tatakelakuan,Panduan Komunikasi Elektronik dan dokumen Dasar Keselamatan Maklumat Global Syarikat, serta mana-mana standard terpakai lain yang dikeluarkan oleh Syarikat dari semasa ke semasa. Semua istilah dalam huruf besar tetapi tidak ditakrifkan dalam Notis ini mempunyai makna seperti yang ditakrifkan dalam dokumen Dasar Keselamatan Maklumat Global Syarikat.

Komunikasi oleh kakitangan Syarikat tertentu yang dikawal selia adalah tertakluk pada syarat penyeliaan tambahan yang terperinci dan Pengguna yang Diberi Kebenaran adalah diingatkan untuk merujuk kepada dasar dan prosedur yang berkenaan bagi bidang perniagaan mereka untuk mendapatkan maklumat lanjut.

Tertakluk kepada undang-undang terpakai, semua Komunikasi Elektronik, termasuk e-mel (sama ada disulitkan[27] atau tidak) dan sambungan kepada laman web Internet dan intranet yang menggunakan sumber pengkomputeran atau rangkaian Syarikat adalah hak milik Syarikat dan mungkin tertakluk pada pemantauan dan pengawasan. Ini termasuk tetapi tidak terhad kepada:

- **Menjalankan aktiviti pemantauan tanpa memberi notis terlebih dahulu ("pemantauan rahsia"), dalam keadaan di mana perlaksanaannya dibenarkan (sebagai contoh sekiranya wujud syak terhadap penyusupan keluar data, aktiviti jenayah atau aktiviti lain yang menyalahi undang-undang atau melanggar Pematuhan Syarikat atau Dasar Keselamatan Maklumat Global atau pelanggaran mana-mana kewajiban lain terhadap Syarikat) atau, apabila diperlukan di bawah undang-undang yang terpakai, di bawah waran atau kebenaran yang berkenaan;**
- **Memantau dan/atau menyekat e-mel yang masuk dan keluar serta pemesejan lain yang ditandakan untuk menunjukkan bahawa ia adalah peribadi atau sulit atau sebaliknya bersifat persendirian sekiranya wujud syak bahawa e-mel sedemikian serta kandungan atau lampirannya bertentangan atau melanggar undang-undang yang terpakai atau Pematuhan Syarikat atau Dasar Keselamatan Maklumat Global atau sebarang kewajiban lain terhadap Syarikat.**

PENGUMPULAN DAN TUJUAN PENGGUNAAN DATA PERIBADI

Aktiviti pemantauan tertentu terhadap sistem dan peranti elektronik Syarikat diamalkan di seluruh Syarikat untuk tujuan yang dinyatakan dalam Lampiran A Notis ini.

Kategori Data Peribadi yang mungkin diproses oleh Syarikat semasa menjalankan pemantauan yang digariskan dalam Notis ini dan asas undang-undang untuk pemprosesan tersebut (termasuk persetujuan, jika perlu) adalah seperti yang dinyatakan dalam DPN yang berkenaan.

Pengguna yang Diberi Kebenaran mungkin mempunyai hak tambahan. Hak Individu, tertakluk kepada

27 Pemantauan dan pengawasan komunikasi yang disulitkan melibatkan penyahsulitan dan penggunaan semula penyulitan.

undang-undang yang terpakai, dinyatakan dalam DPN yang berkaitan. (Bahagian VII: Akses, Kemudahalihan, Pembetulan dan Pembatasan, Had dan Sekatan Pemprosesan dan Ketepatan Data Peribadi).

Syarikat berhak, tertakluk kepada undang-undang yang terpakai dan tanpa notis lanjut, untuk menggunakan pemantauan data yang dipertingkatkan pada komputer dan/atau peranti mudah alih anda yang disediakan oleh bank dalam keadaan tertentu (termasuk tetapi tidak terhad kepada anda yang mempunyai keistimewaan dan akses yang lebih tinggi atau tarikh akhir bekerja yang semakin hampir).

DATA PERIBADI SENSITIF

Syarikat boleh mengumpul dan memproses Data Peribadi tertentu dalam kategori khusus termasuk Data Peribadi Sensitif, seperti yang dinyatakan dalam DPN yang berkenaan, semasa menjalankan aktiviti yang dijelaskan dalam Notis ini.

Aktiviti pemantauan Keselamatan Maklumat Global tidak memantau secara aktif Data Peribadi Sensitif, namun sesetengah Data Peribadi Sensitif mungkin akan didedahkan semasa memantau jenis data lain.

AKSES OLEH KAKITANGAN SYARIKAT

Akses kepada data peribadi yang diproses menurut notis ini adalah terhad kepada individu yang memerlukan akses sedemikian untuk tujuan yang disenaraikan dalam DPN yang berkenaan termasuk tetapi tidak terhad kepada ahli pasukan Keselamatan Maklumat Global dan Penyiasatan Perusahaan Dalaman dalam bidang kuasa tempatan Pengguna yang Diberi Kebenaran dan/atau bidang kuasa lain di mana Syarikat beroperasi.

PENDEDAHAN

Alat dan proses pemantauan yang dijelaskan dalam Notis ini boleh digunakan oleh pasukan Keselamatan Maklumat Global Syarikat dan mana-mana sekutu dan cawangannya termasuk yang berada di A.S., U.K., Singapura, Hong Kong dan India serta di negara/rantau beroperasi tertentu. Data Peribadi boleh disimpan dan/atau diproses di bidang kuasa tempatan Pengguna yang Diberi Kebenaran dan/atau bidang kuasa lain di mana Syarikat beroperasi.

Memandangkan sifat global aktiviti Syarikat, Syarikat boleh memindahkan Data Peribadi anda ke negara-negara yang terletak di luar negara asal anda, seperti yang dinyatakan dalam DPN yang berkenaan.

Syarikat boleh mendedahkan, mengikut undang-undang yang terpakai, Data Peribadi yang berkaitan kepada mana-mana anggota sekutu dan cawangannya dan mereka boleh memproses Data Peribadi tersebut untuk tujuan yang dinyatakan dalam Notis ini. Selain itu, Syarikat boleh mendedahkan, mengikut undang-undang yang terpakai, Data Peribadi yang berkaitan kepada pihak ketiga tertentu seperti yang dinyatakan dalam DPN yang berkenaan.

KESELAMATAN

Syarikat mengambil langkah-langkah teknikal dan organisasi yang bersesuaian untuk melindungi daripada

pemprosesan Data Peribadi yang tidak dibenarkan atau menyalahi undang-undang dan/atau terhadap kehilangan secara tidak sengaja, pengubahan, pendedahan atau akses, atau pemusnahan atau kerosakan Data Peribadi yang tidak disengajakan atau menyalahi undang-undang.

MODUS PEMPROSESAN DAN PENGEKALAN DATA

Semua aktiviti pemantauan dan pengawasan pada mulanya tidak menyasarkan individu tertentu. Pengguna yang Diberi Kebenaran hanya akan dikenal pasti sekiranya terdapat tanda-tanda penyalahgunaan atau kelakuan yang mencurigakan, mengikut tujuan yang dinyatakan dalam Notis ini. Sekiranya penggunaan peribadi sistem bank mengakibatkan komunikasi peribadi yang perlu disemak, sebarang semakan tersebut akan dijalankan selaras dengan undang-undang, peraturan dan garis panduan yang berkenaan.

Apabila memproses Data Peribadi untuk tujuan yang dinyatakan dalam Notis ini, Syarikat tidak menggunakan pembuatan keputusan secara automatik terhadap proses-proses Pengguna yang Diberi Kebenaran di mana keputusan tersebut akan mempunyai kesan undang-undang atau kesan ketara yang serupa terhadap Pengguna yang Diberi Kebenaran apabila melaksanakan pemantauan seperti yang diterangkan dalam Notis ini. ‘Membuat keputusan automatik’ ialah proses membuat keputusan secara automatik tanpa penglibatan mana-mana manusia.

Tempoh pengekalan bagi setiap jenis data dan bidang kuasa digariskan dalam Jadual Pengekalan Rekod Global yang terdapat di halaman Pengurusan Rekod Global di Flagscape. Senarai keperluan pengekalan disediakan atas permintaan untuk Pengguna yang Diberi Kebenaran yang baharu, yang belum mempunyai akses ke laman web dalaman. Syarikat akan memadamkan Data Peribadi selepas tempoh pengekalan yang berkenaan.

TINDAKAN DISIPLIN

Pengguna yang Diberi Kebenaran yang melanggar mana-mana polisi yang dirujuk dalam Notis ini mungkin tertakluk pada penyiasatan, penggantungan akses dan/atau prosiding disiplin (sehingga dan termasuk pemberhentian pekerjaan atau perkhidmatan kontrak). Pengguna yang Diberi Kebenaran yang bukan pekerja boleh dirujuk kepada majikan mereka untuk tindakan disiplin. Pengguna yang Diberi Kebenaran yang melanggar undang-undang atau peraturan yang terpakai boleh dirujuk kepada penguat kuasa undang-undang dan/atau pegawai kawal selia mengikut keperluan undang-undang dan pengawalseliaan. Sebarang bahan atau bukti yang dikenal pasti dengan cara (termasuk tetapi tidak terhad kepada) pemantauan panggilan telefon, e-mel dan penggunaan Internet atau intranet (termasuk panggilan telefon, e-mel dan penggunaan Internet secara peribadi) boleh digunakan dalam sebarang prosiding disiplin dan penyiasatan dalaman atau luaran. Pengguna yang Diberi Kebenaran dikehendaki untuk bekerjasama dalam pertanyaan, pemeriksaan, pemantauan dan aktiviti rakaman jika diminta. Keengganan untuk bekerjasama dalam siasatan keselamatan boleh menyebabkan tindakan undang-undang atau disiplin, termasuk penamatan pekerjaan atau perkhidmatan kontrak.

BUTIRAN HUBUNGAN

Untuk pertanyaan atau maklumat lanjut mengenai Notis ini atau aktiviti pemantauan Keselamatan Maklumat Global, Pengguna yang Diberi Kebenaran hendaklah menghubungi Keselamatan Maklumat

Global.

Anda mungkin mempunyai hak untuk membuat aduan kepada Pihak Berkuasa Perlindungan Data untuk negara anda. Untuk kesesuaian dan maklumat lanjut, rujuk DPN yang berkenaan.

Untuk soalan mengenai undang-undang dan sekatan tempatan, Pengguna yang Diberi Kebenaran hendaklah menghubungi pegawai pematuhan tempatan mereka, Pegawai Perlindungan Data atau jabatan undang-undang.

PINDAAN TERHADAP NOTIS INI

Notis ini tidak bersifat kontraktual dan Syarikat berhak untuk meminda atau menarik balik Notis pada bila-bila masa. Sekiranya Syarikat membuat perubahan besar terhadap Notis ini, Syarikat akan memaklumkan Pengguna yang Diberi Kebenaran dengan secepat mungkin yang munasabah dengan mengeluarkan semula Notis yang dipinda dan/atau mengambil langkah-langkah lain mengikut undang-undang yang terpakai.

LAMPIRAN A

Rujuk matriks yang dipautkan di sini untuk melihat kategori data yang boleh dikumpulkan bagi setiap tujuan penggunaan, yang diringkaskan di bawah. Matriks tersebut disediakan atas permintaan untuk Pengguna yang Diberi Kebenaran yang baharu, yang belum mempunyai akses ke laman web dalaman.

Komunikasi dan Rekod (sama ada secara langsung atau selepas peristiwa tersebut berlaku) yang kami pantau pada sistem dan peranti elektronik Syarikat dan yang kami mungkin gunakan untuk mengumpul Data Peribadi termasuk, tetapi tidak terhad kepada:

- E-mel yang dihantar;
- E-mel yang diterima;
- Penggunaan web / internet, FTP, HTTP, HTTPS, Telnet;
- Penggunaan dan kandungan cetakan;
- Fail yang terdapat dalam komputer meja (di luar My Documents), laman-laman kolaborasi, perkongsian terbuka, Wiki dalaman;
- Media boleh alih, peranti yang Tidak Diuruskan Syarikat yang bersambung dengan sistem Syarikat;
- Pemesejan segera;
- Panggilan telefon, panggilan VOIP, mel suara;
- Akses aplikasi dan log serta rekod penggunaan;
- Maklumat capaian rangkaian (termasuk alamat IP dan ISP);
- Akses ke sistem dan log serta rekod penggunaan (termasuk rekod yang menunjukkan corak penggunaan dan pengendalian);
- Faks dan Pengimbasan/Pengimejan Dokumen;
- Penggunaan dan kandungan media sosial (luaran, bukan Syarikat);
- Sumber terbuka dan maklumat yang tersedia secara umum;
- Log keselamatan;
- Log utama dan tangkapan skrin;

- Teknologi persidangan;
- Kuki, Beacon, Sinkhole dan Honeypot;
- Data Geolokasi[28]
- Data kemasukan Kad Leret;
- Mesej Teks yang dihantar dan diterima.

TUJUAN KAMI MENGUMPUL, MENGGUNAKAN, MEMINDAHKAN DAN MENDEDAHKAN DATA PERIBADI:

Dasar Keselamatan Maklumat Global adalah bertujuan untuk menyediakan keperluan penting untuk membolehkan Syarikat menyediakan, mencegah, mengesan, bertindak balas dan mengambil langkah pemulihan terhadap perubahan landskap ancaman yang meningkat. Program Keselamatan Maklumat Global menyediakan penyelesaian dan menggunakan teknik lanjutan untuk menghalang ancaman keselamatan maklumat daripada menjejaskan keyakinan pelanggan dan mengganggu operasi perniagaan. Keselamatan Maklumat Global melindungi Syarikat dan pelanggannya dengan menggunakan rangka kerja berasaskan risiko dan tertumpu pada hasil.

- Sediakan: Kami melindungi dengan mengemas kini secara berterusan Program Keselamatan Maklumat yang termasuk mematuhi undang-undang tempatan atau asing dan/atau yang khusus kepada negara untuk menjangkakan dan mengenal pasti potensi ancaman dengan lebih berkesan;
- Cegah: Kami melindungi dengan kekal mendahului musuh melalui penggunaan kawalan pencegahan untuk mengelakkan kehilangan, penyalahgunaan dan penggunaan tidak wajar maklumat sulit dan proprietari serta mengurangkan bilangan insiden;
- Kesan: Kami melindungi dengan mengehadkan pendedahan melalui penggunaan kawalan pengesanan termasuk pemantauan tembok api, perlindungan antispam dan virus serta pemantauan lain; pemantauan berterusan terhadap semua rakan sepasukan bank, aplikasi, data, sistem dan rangkaian;
- Kurangkan: Kami melindungi dengan mengurangkan insiden dengan menggunakan keupayaan tindak balas yang tangkas dan selaras;
- Tindak Balas/Pulih: Kami melindungi dengan meningkatkan kedudukan keselamatan dengan menggunakan keupayaan forensik yang mantap, penyiasatan dan pembelajaran di samping menangani sebarang masalah pematuhan, pertanyaan siasatan kawal selia, tindakan disiplin atau tuntutan undang-undang.

[28] Data geolokasi ditakrifkan sebagai data yang diambil daripada peranti pengguna yang menunjukkan lokasi geografi peranti tersebut, termasuk data GPS atau data mengenai sambungan dengan peralatan wifi tempatan