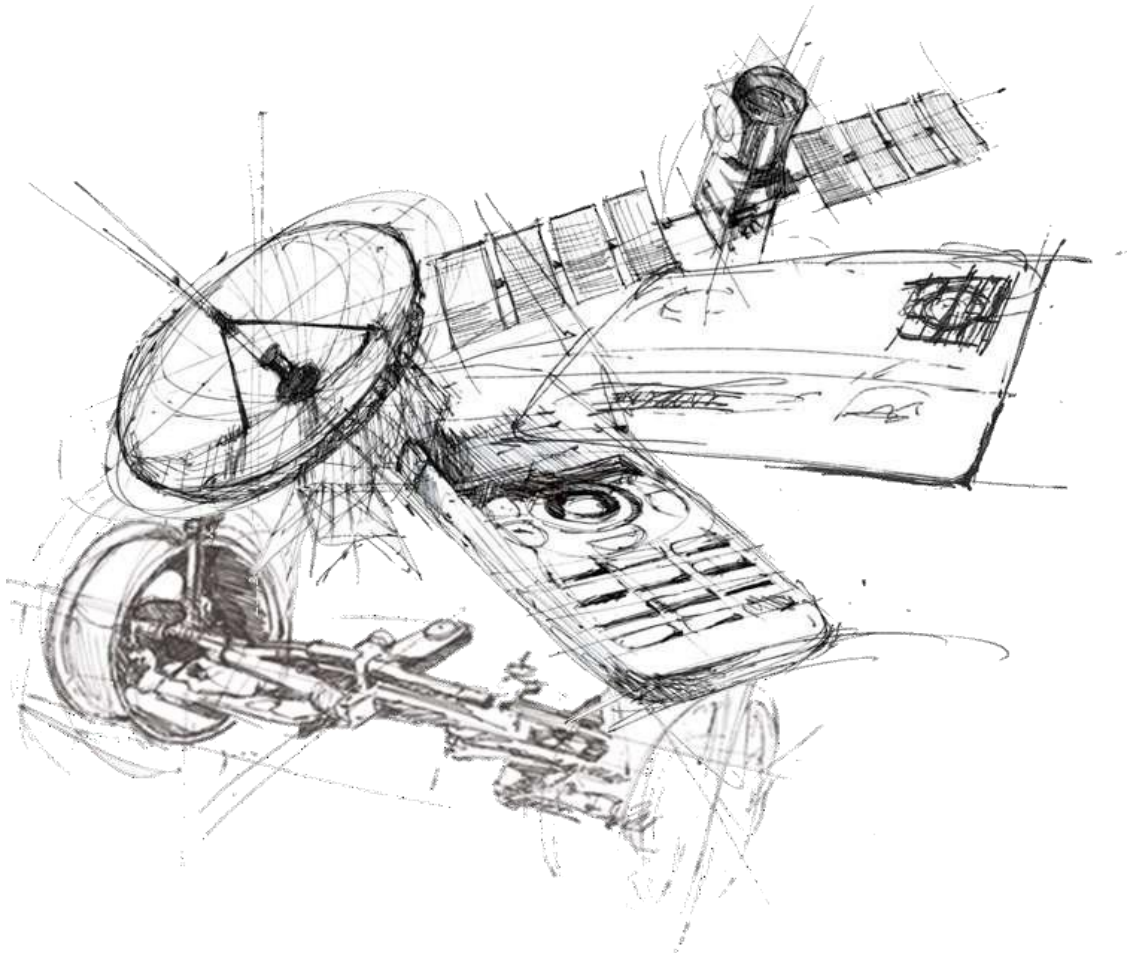
ALTEN Group's Security Requirements

Yêu Cầu Bảo Mật Của Tập Đoàn ALTEN



1. PURPOSE/*MỤC ĐÍCH*

The ALTEN Group, aware of its obligation to ensure a high level of security for its business activities and those of its client projections, is responsible for making sure that activities entrusted to third parties, partners or sub-contractors are executed in accordance with the conditions of availability, integrity, confidentiality and traceability imposed by the legal and contractual obligations of its business.

Tập đoàn ALTEN, với nhận thức sâu sắc về trách nhiệm trong việc đảm bảo mức độ an ninh cao trong hoạt động kinh doanh cũng như các dự án thực hiện cho khách hàng, cam kết rằng mọi hoạt động được ủy thác cho bên thứ ba, đối tác hoặc nhà thầu phụ đều phải tuân thủ nghiêm ngặt các tiêu chí về tính khả dụng, toàn vẹn, bảo mật và khả năng truy xuất phù hợp với các yêu cầu pháp lý và cam kết hợp đồng đã đề ra.

In this context, the ALTEN Group specifies the security requirements that the Service Provider must meet with a performance obligation. These security requirements include sections related to organisation security, the physical security of premises, information security, awareness raising, and business continuity.

Trong bối cảnh này, Tập đoàn ALTEN đặt ra các yêu cầu bảo mật cụ thể mà Nhà Cung Cấp phải đáp ứng theo nghĩa vụ thực hiện. Các yêu cầu bảo mật này bao gồm những nội dung liên quan đến an tinh tổ chức, an ninh vật lý tại cơ sở, đảm bảo an toàn thông tin, nâng cao nhận thức về an ninh và duy trì hoạt động trong mọi tình huống.

In response to these requirements, and in accordance with the contract, the Service Provider is likely to produce the Security File describing the security measures implemented, as well as the application methods depending on the field of activity concerning it.

Để đáp ứng đầy đủ các yêu cầu này và tuân thủ các quy định tại hợp đồng, Nhà Cung Cấp có thể cần tạo dựng Thư mục Bảo mật – được hiểu là tài liệu mô tả chi tiết các biện pháp bảo mật được triển khai, cũng như các biện pháp ứng dụng cụ thể tùy vào lĩnh vực hoạt động có liên quan.

2. SCOPE/*PHẠM VI*

This document defines all the ALTEN Group's security requirements and applies to all ALTEN Group Service Providers.

Tài liệu này quy định toàn bộ yêu cầu bảo mật của Tập đoàn ALTEN và áp dụng cho tất cả Nhà Cung Cấp của Tập đoàn.

3. ASSOCIATED DOCUMENTS/*CÁC TÀI LIỆU LIÊN QUAN*

Reference *Tham chiếu*	Description *Mô tả*
EPO-GRI-003	General Information Systems Security Policy *Chính sách chung về Bảo mật hệ thống thông tin*
EPO-GRI-025	Operational Policy for the Management of Third Parties *Chính sách về Vận hành về quản lý Bên Thứ Ba*
EPO-GRI-005	ALTEN Group Information Processing Policy *Chính sách xử lý thông tin của Tập đoàn ALTEN*

SMSI documents (process, sub-process, procedures, guides and forms) are stored on the ALTEN Group's document base or in the ISO27001 standard.

Các tài liệu thuộc Hệ thống Quản lý An toàn Thông tin (SMSI) (bao gồm: quy trình, quy trình con, thủ tục, hướng dẫn, biểu mẫu) được lưu trữ trên cơ sở dữ liệu của Tập đoàn ALTEN hoặc theo tiêu chuẩn ISO27001.

4. DEFINITIONS/ĐỊNH NGHĨA

Terms *Từ ngữ*	Definitions *Định nghĩa*
ISOC	Information Security Officer Correspondent *Cán bộ Phụ trách An toàn Thông tin*
SAP	Security Assurance Plan, also referred to in this document as a "security file". Kế hoạch Đảm bảo An ninh, còn được gọi trong tài liệu này là "Thư mục bảo mật".
Service Provider	Any person or business performing services for one of the ALTEN Group companies, as identified in Article 10 of this document. *Bất kỳ các cá nhân hoặc tổ chức nào thực hiện thực hiện dịch vụ cho một trong các công ty thuộc Tập đoàn ALTEN, được quy định tại Điều 10 của tài liệu này.*
IS	Information System *Hệ thống Thông tin*
CISO	Chief Information Security Officer *Giám đốc phụ trách mảng An toàn Thông tin*
ALTEN Group *Tập đoàn ALTEN*	Any company which, directly or indirectly, controls, is controlled by, or is under the common control of ALTEN SA within the meanings of Articles L. 233-1 and following the Code of Commerce. *Bất kỳ công ty nào, trực tiếp hoặc gián tiếp bị kiểm soát hoặc chịu sự kiểm soát chung với ALTEN SA theo quy định tại Điều L.233-1 và các điều khoản khác của Luật Thương Mại.*

5. CLASSIFICATION OF SERVICES/*PHÂN LOẠI DỊCH VỤ*

TYPE OF SERVICES *LOẠI DỊCH VỤ*	DETAILS *CHI TIẾT*	REF. *THAM CHIẾU*	APPLICABLE REQUIREMENTS *YÊU CẦU ÁP DỤNG*
Equipment Maintenance ***Bảo trì thiết bị***	Equipment maintenance services *Dịch vụ bảo trì thiết bị*	01	7.2 – 7.5 – 7.7 8.1 – 8.3 9.1 to 9.14
Software Maintenance ***Bảo trì phần mềm***	Software maintenance services *Dịch vụ bảo trì phần mềm*	02	7.1 – 7.2 – 7.3 7.4 – 7.6 – 7.7 8.2 9.1 à 9.14
Purchase of equipment ***Mua sắm thiết bị***	Purchase services of IT equipment *Dịch vụ mua sắm thiết bị Công nghệ thông tin (CNTT)*	03	9.1 to 9.14
Purchase of software licences ***Mua bản quyền phần mềm***	Purchase services of software licences *Dịch vụ mua bản quyền phần mềm*	04	9.1 to 9.14

Recovery of data back-up/Disposal ***Phục hồi dữ liệu sao y/ Hủy dữ liệu***	Data back-up recovery services and/or disposal services and/or equipment donations *Dịch vụ khôi phục dữ liệu sao lưu và/hoặc hủy dữ liệu và/hoặc trao tặng thiết bị*	05	7.1 – 7.2 – 7.5 8.1 9.1 to 9.14
Remote maintenance/Remote administration ***Bảo trì từ xa/Quản trị từ xa***	Remote maintenance and/or administration services via a means of communication (local network, Internet) *Dịch vụ bảo trì và/hoặc quản trị từ xa thông qua các phương tiện truyền thông (như mạng nội bộ, Internet)*	06	7.1 – 7.2 – 7.3 7.5 – 7.6 – 7.7 9.1 to 9.14
Network Interconnection ***Kết nối mạng***	Services requiring interconnection with the ALTEN network *Các dịch vụ yêu cầu kết nối mạng với mạng nội bộ của ALTEN*	07	7.1 – 7.2 – 7.3 7.5 – 7.6 – 7.7 9.1 to 9.14
Audit/Advice/Expertise ***Kiểm toán/Tư vấn/Chuyên gia***	Audit, advisory and/or expert services *Dịch vụ kiểm toán, tư vấn và/hoặc dịch vụ hỗ trợ từ chuyên gia*	08	7.1 – 7.2 – 7.5 7.6 – 8.2 9.1 to 9.14
Software and/or application development ***Phát triển phần mềm và/hoặc phát triển ứng dụng***	Software and/or application development services *Dịch vụ phát triển phần mềm và/hoặc phát triển ứng dụng*	09	7.1 – 7.2 – 7.4 7.5 – 7.6 – 7.7 9.1 to 9.14
Installation/Integration/ Deployment ***Lắp đặt/Tích hợp/Triển khai***	Installation, integration and/or IT solution deployment services *Dịch vụ cài đặt, tích hợp và hoặc triển khai giải pháp công nghệ thông tin (CNTT)*	10	7.1 – 7.2 – 7.5 8.1 – 8.2 9.1 to 9.14
Outsourcing ***Dịch vụ thuê ngoài***	Outsourcing services for the management of all of part of the information system *Dịch vụ gia công phần mềm quản lý hệ thống thông tin (một phần hoặc toàn bộ)*	11	7.1 – 7.2 – 7.3 7.5 – 7.6 – 7.7 7.8 – 8.2 – 8.3 9.1 to 9.14
Monitoring ***Giám sát***	Services monitoring the availability of servers or IT equipment *Các dịch vụ giám sát tính khả dụng của máy chủ hoặc thiết bị công nghệ thông tin (CNTT)*	12	7.1 – 7.2 – 7.3 8.2 – 8.3 9.1 to 9.14
Hosting ***Lưu trữ dữ liệu***	Server and/or application and/or data hosting services *Dịch vụ lưu trữ hạ tầng máy chủ, ứng dụng và dữ liệu*	13	7.1 – 7.2 – 7.3 7.5 – 7.6 – 7.7 7.8 – 8.2 – 8.3 9.1 to 9.14

Cloud (SaaS, IaaS, PaaS)	Remote network, server, application and service hosting services via a telecommunications network *Dịch vụ lưu trữ mạng từ xa, máy chủ, ứng dụng và dịch vụ qua mạng viễn thông*	14	7.1 – 7.2 – 7.3 7.5 – 7.6 – 7.7 7.8 – 8.2 – 8.3 9.1 to 9.14
Site operation	Services giving rise to operating, security, monitoring, hosting or on-site maintenance activities related to General Resources. *Các dịch vụ liên quan đến hoạt động vận hành, bảo mật, giám sát, lưu trữ hoặc bảo trì tại chỗ liên quan đến tài nguyên chung.*	15	7.2 – 7.5 – 7.7 8.1 9.1 to 9.14

6. GENERAL ISSUES/*VẤN ĐỀ CHUNG*

The ALTEN Group's security referential is ISO27001. The implementation and control measures imposed on Service Providers are based on ISO27002.

Tập đoàn ALTEN áp dụng tiêu chuẩn ISO27001 làm bộ quy chuẩn về bảo mật thông tin. Các biện pháp triển khai và kiểm soát áp dụng đối với Nhà Cung Cấp được áp dụng dựa trên tiêu chuẩn ISO27002.

Generally, the ALTEN Group requests that its Service Providers respect the ISO27001 international standard. ISO27001 outlines the general principles for achieving information literacy across a specific management system.

Nhìn chung, Tập đoàn ALTEN yêu cầu các Nhà Cung Cấp phải tuân thủ tiêu chuẩn quốc tế ISO27001- bộ tiêu chuẩn đặt ra những nguyên tắc tổng quát nhằm đạt được sự am hiểu về thông tin trong một hệ thống quản lý cụ thể.

In particular, it must be applied in cases where services are performed remotely on ALTEN Group information systems.

Tiêu chuẩn này đặc biệt cần áp dụng trong các trường hợp dịch vụ được thực hiện từ xa trên các hệ thống thông tin của Tập đoàn ALTEN.

The ALTEN Group has a framework of Information System (IS) Security Policies outlining the expected level of security to be implemented during services.

Tập đoàn ALTEN đã xây dựng Chính sách về bảo mật hệ thống thông tin, trong đó nêu rõ cấp độ an toàn thông tin cần được thực hiện trong suốt quá trình cung cấp dịch vụ.

The Service Provider undertakes to respect all of the security requirements outlined in this document during the execution of these services.

Nhà Cung Cấp cam kết tuân thủ các yêu cầu bảo mật được quy định trong văn bản này trong suốt quá trình thực hiện dịch vụ.

The Service Provider recognises that he is obliged to advise, alert and offer recommendations in terms of security and the state of the art. His is committed, in particular, the informing the ALTEN Group of any risks identified in the services that he is providing.

Nhà Cung Cấp thừa nhận họ có trách nhiệm tư vấn, cảnh báo và đưa ra các khuyến nghị phù hợp về mặt an ninh và các giải pháp công nghệ tiên tiến nhất. Đặc biệt, họ cam kết thông báo cho Tập đoàn ALTEN về mọi rủi ro được xác định đối với dịch vụ mà họ cung cấp.

7. SECURITY REQUIREMENTS RELATED TO INFORMATION SYSTEMS (IS)/*CÁC YÊU CẦU BẢO MẬT LIÊN QUAN ĐẾN HỆ THỐNG THÔNG TIN*

7.1 RULES RELATED TO THE PROVIDER'S IS
CÁC QUY TẮC LIÊN QUAN ĐẾN HỆ THỐNG THÔNG TIN CỦA NHÀ CUNG CẤP

PIS1: Information backups of ALTEN Group data and/or information are made regularly, and stored on a secure backup site or stored in a waterproof and fireproof safe in the case of physical backups.
***PIS1**: Dữ liệu và/hoặc thông tin của Tập đoàn ALTEN được sao lưu định kỳ và lưu trữ tại một điểm sao lưu an toàn, hoặc trong trường hợp sao lưu vật lý thì sẽ được bảo quản trong két chống cháy và chống nước.*

PIS2: The Service Provider's information system benefits from an autonomous emergency power supply, compliant with the commitment to meet the needs of conventions and the level of service defined in the contract.
***PS2**: Hệ thống thông tin của Nhà Cung Cấp được trang bị nguồn cung cấp điện khẩn cấp tự động, đảm bảo đáp ứng các yêu cầu theo cam kết và mức độ dịch vụ đã được quy định tại hợp đồng.*

PIS3: The information system must be protected against physical intrusions from outside and against internal malicious acts.
***PS3**: Hệ thống thông tin phải được bảo vệ khỏi sự xâm nhập vật lý từ bên ngoài và các hành vi phá hoại trong nội bộ.*

***PIS4**: The information system must be protected against viral attacks and computer intrusions/attacks.*
***PIS4**: Hệ thống thông tin phải được bảo vệ khỏi các cuộc tấn công bằng virus và các hình thức tấn công/xâm nhập hệ thống máy tính.*

PIS5: The Service Provider must ensure that security equipment vulnerabilities are monitored and apply corrective measures to the server, workstation, equipment and application operating systems.
***PIS5**: Nhà Cung Cấp phải theo dõi các lỗ hổng của thiết bị bảo mật và tiến hành triển khai các biện pháp khắc phục đối với hệ điều hành của máy chủ, máy trạm, thiết bị và hệ điều hành ứng dụng.*

PIS6: The information and/or data of the ALTEN Group or its clients, hosted on the Service Provider's IS, must only be accessed for the purposes of completing Services (control of access to applications and devices, etc.).
***PIS6**: Thông tin và/hoặc dữ liệu của Tập đoàn ALTEN hoặc của khách hàng của Tập đoàn được lưu trữ trên hệ thống thông tin của Nhà Cung Cấp, chỉ được truy cập nhằm mục đích hoàn thành các Dịch Vụ (kiểm soát truy cập vào ứng dụng và thiết bị, v.v).*

PIS7: The procedures for exchanging information must make it possible to ensure the confidentiality and integrity of ALTEN Group information and data, and authenticate the entities/parties in communication. Exchanges of information are therefore systematically encrypted in a way that respects the current rules of good practice recommended by ANSSI.
***PIS7**: Các quy trình trao đổi thông tin phải được đảm bảo tính bảo mật và toàn vẹn của dữ liệu thuộc Tập đoàn ALTEN, đồng thời xác thực rõ ràng các bên tham gia trao đổi. Do đó, mọi thông tin trao đổi đều phải được mã hóa một cách có hệ thống bằng cách tôn trọng các quy tắc hiện hành được khuyến nghị bởi Cơ quan An ninh mạng và Thông tin Quốc gia Pháp (ANSSI).*

PIS8: If encryption tools ("encrypting") must be implemented, the methods used must be authorised by French law. They must use strong cryptographic methods. For this reason, a 3DE or AES encryption device, with a key length of 128/256 bits, must be used as a minimum.
***PIS8**: Nếu cần triển khai công cụ mã hóa ("mã hóa"), thì việc sử dụng phương pháp này phải được cho phép theo quy định pháp luật Pháp và phải sử dụng các thuật toán mã hóa mạnh. Với lý do này, tối thiểu cần sử dụng thiết bị mã hóa 3DE hoặc AES, với độ dài khóa là 127/256 bits.*

PIS9: The decryption keys are only communicated to person who have signed a confidentiality agreement. In this agreement, these persons agree not to disclose the keys.
***PIS9**: Các khóa giải mã chỉ được cung cấp cho các cá nhân đã ký cam kết bảo mật thông tin. Trong thỏa thuận này, các cá nhân không được phép tiết lộ các khóa giải mã.*

PIS10: ALTEN Group data and/or information must not be duplicated or transmitted to a third-party without the prior written approval of the ALTEN Group.
***PIS10**: Dữ liệu và/hoặc thông tin của Tập đoàn ALTEN không được phép sao chép hay chuyển giao cho bất kỳ bên thứ ba nào mà chưa có sự đồng ý bằng văn bản của Tập đoàn.*

PIS11: The ALTEN Group information, data and files stored on the Service Provider's IS must be physically and irreversibly deleted from the data carriers after the Services have been completed, including any back up devices.

***PIS11**: Tất cả mọi thông tin, dữ liệu của Tập đoàn ALTEN được lưu trữ trên hệ thống thông tin của Nhà Cung Cấp phải được xóa hoàn toàn, vĩnh viễn và không thể khôi phục được khỏi các thiết bị lưu trữ, bao gồm các thiết bị sao lưu sau khi Dịch Vụ được hoàn thành.*

PIS12: Any transfer of files relating to Services on a physical device (DAT, CD ROM...) by an external courier or holder requires acknowledgement of receipt. The rules for the protection of information and documents outlined in the ALTEN Group's information processing policy must be respected.
***PIS12**: Mọi việc chuyển giao các thư mục liên quan đến dịch vụ thông qua thiết bị vật lý (như DAT, CD ROM…) được thực hiện bởi người hoặc đơn vị vận chuyển bên ngoài đều phải có biên bản xác nhận. Các quy tắc về bảo mật thông tin và tài liệu được nêu trong chính sách xử lý thông tin của Tập đoàn ALTEN phải được tuân thủ.*

7.2 QUALIFICATION AND EXPERIENCE IN THE ISS FIELD
TRÌNH ĐỘ VÀ KINH NGHIỆM TRONG LĨNH VỰC BẢO MẬT HỆ THỐNG THÔNG TIN (ISS)

ART01: The Service Provider must justify:
***Điều 01:** Nhà Cung Cấp phải chứng minh:*

- the qualifications and certifications of his employees completing the Services;
  trình độ chuyên môn và chứng chỉ của nhân sự thực hiện Dịch Vụ;
- the frequency and content of his employees' training and awareness raising related to security issues.
  tần suất và nội dung các chương trình đào tạo, nâng cao nhận thức về an ninh cho nhân viên của mình.

ART02: The ALTEN Group can ask the Service Provider to carry out a criminal background check on his employees.
***Điều 02:** Tập đoàn ALTEN có thể yêu cầu Nhà Cung Cấp thực hiện kiểm tra lý lịch tư pháp đối với nhân viên của mình.*

7.3 REMOTE ACCESS MANAGEMENT
QUẢN LÝ TRUY CẬP TỪ XA

REM1: Remote accesses to the ALTEN Group IS must pass through a Service Provider focal point, dedicated to the Service Providers, and be strictly limited to the Service Provider's employees. These accesses must also be limited to the strict time duration of the Services (unless documented and approved by the ALTEN Group COSI).
***REM1**: Mọi truy cập từ xa vào hệ thống thông tin (IS) của Tập đoàn ALTEN phải đi qua một đầu mối chuyên trách dành riêng cho các Nhà Cung Cấp và chỉ giới hạn cho nhân sự của Nhà Cung Cấp. Các quyền truy cập này cũng bị giới hạn trong khoảng thời gian thực hiện Dịch Vụ (trừ khi có tài liệu nào chứng minh và được Ban vận hành an toàn thông tin của Tập đoàn phê duyệt).*

REM2: The ALTEN Group IS must be accessed with the help of an individual nominative account. Individualisation of an account consists of associating an account with a single physical person for a time-limited duration. In the case of necessity (request from authorities, case of malice), the Service Provider must be able to reveal the identity of the person using an account at a given time.
***REM2**: Việc truy cập vào hệ thống thông tin của Tập đoàn ALTEN phải được thực hiện thông qua tài khoản định danh cá nhân. Việc cá nhân hóa tài khoản bao gồm việc liên kết tài khoản với một cá nhân cụ thể trong việc khoảng thời gian được giới hạn. Trong trường hợp cần thiết (theo yêu cầu từ các cơ quan chức năng, hoặc trong các trường hợp có hành vi cố ý gây hại), Nhà Cung Cấp phải có khả năng tiết lộ danh tính của người đang sử dụng tài khoản tại bất kỳ thời điểm nào.*

REM3: The Service Provider undertakes to only use the logical access accounts and the potential associated methods (multi-factor authentication) expressly entrusted to him by the ALTEN Group for this purpose.
***REM3**: Nhà Cung Cấp cam kết chỉ sử dụng các tài khoản truy cập hệ thống và các phương thức liên quan (như: xác thực đa yếu tố) được Tập đoàn ALTEN giao phó rõ ràng cho mục đích này.*
REM4: This Service Provider must ensure the security and traceability of authentication elements transmitted by the ALTEN Group.
***REM4**: Nhà Cung Cấp phải đảm bảo tính bảo mật và khả năng truy xuất các yếu tố xác thực được Tập đoàn ALTEN cung cấp.*

REM5: The Service Provider's workstations must not, in any case, allow a rebound between the ALTEN Group network and third-party network. It is especially prohibited, for the full time that a Service Provide workstation is connected to an ALTEN Group network, to connect the Service Provider device, regardless of the type of device, to another network (via a dual network router, modem, gateway between LAN and WiFi, etc...).
***REM5**: Trong bất cứ trường hợp nào, các máy trạm của Nhà Cung Cấp tuyệt đối không được phép tạo cầu nối giữa mạng nội bộ của Tập đoàn với mạng của bên thứ ba. Đặc biệt, nghiêm cấm thực hiện, trong toàn bộ thời gian mà máy trạm của Nhà Cung Cấp được kết nối với mạng của ALTEN, đối với việc kết nối thiết bị của Nhà Cung Cấp bất kể loại thiết bị nào với một mạng khác (thông qua bộ định tuyến mạng kép, bộ điều giải, cổng kết nối mạng giữa LAN và WiFi, v.v).*

REM6: The Service Provider's workstations must connect to the ALTEN Group network by the methods approved by the ALTEN Group before the implementation of the Services, and through an encrypted protocol (VPN, encrypted flow, VLAN, etc.).
***REM6**: Các máy trạm của Nhà Cung Cấp chỉ được phép kết nối với mạng nội bộ của Tập đoàn ALTEN bằng các phương thức đã được Tập đoàn phê duyệt trước tiến hành Dịch Vụ, và thông qua các giao thức mã hóa (như: VPN, luồng mã hóa dữ liệu, VLAN, v.v).*

REM7: All flows (source and recipient addresses, ports, flow direction) that must be open between the ALTEN Group's and the Service Provider's networks must be documented by the Service Provider (methods, tools used to connect to the ALTEN Group network or to an application).
***REM7**: Tất cả các luồng dữ liệu (như: địa chỉ nguồn, đích, cổng và hướng truyền dữ liệu) được kết nối giữa mạng của Tập đoàn ALTEN và mạng của Nhà Cung Cấp phải được Nhà Cung Cấp ghi lại đầy đủ (thông qua các phương pháp, công cụ để kết nối với mạng lưới của Tập đoàn ALTEN hoặc với một ứng dụng).*

REM8: Service Provider workstations accessing an ALTEN Group network must be configured with a minimum acceptable security level in relation to the ALTEN Group security requirements defined in this document, concerning, in particular, the hardening of OSs, anti-virus, the firewall, the management of security patches, keeping applications and modules (Java, .net, etc.) up to date.
***REM8**: Các máy trạm của Nhà Cung Cấp mà truy cập vào mạng lưới của Tập đoàn ALTEN phải được cấu hình với mức độ bảo mật tối thiểu được chấp nhận theo các yêu cầu bảo mật của Tập đoàn ALTEN được xác định trong văn bản này, điều này đặc biệt liên quan đến việc tăng cường bảo mật hệ điều hành (OS), phần mềm diệt vi-rút, tường lửa, quản lý các bản vá bảo mật và cập nhật các ứng dụng mô-đun (Java., net, v.v).*

REM9: All operations carried out remotely on the ALTEN Group IS by Service Provider personnel must be tracked, attributed to the authors (and not to an IP) and time-stamped on the Service Provider's systems.
***REM9**: Tất cả các thao tác được thực hiện từ xa trên Hệ thống Thông tin của Tập đoàn ALTEN bởi nhân sự của Nhà Cung Cấp phải được theo dõi, xác định rõ người thực hiện (thay chỉ ghi lại địa chỉ IP) và phải đánh dấu thời gian trên hệ thống của Nhà Cung Cấp.*

7.4 SOFTWARE DEVELOPMENT
PHÁT TRIỂN PHẦN MỀM

DEV1: The Service Provider is responsible for ensuring the security of the developments that he has carried out as part of the Services, compliant with state of the art in each of the technologies implemented.
***DEV1**: Nhà Cung Cấp có trách nhiệm đảm bảo vấn đề an ninh cho các hạng mục phát triển phần mềm do mình thực hiện trong phạm vi cung cấp Dịch vụ, phù hợp với các giải pháp công nghệ tiên tiến nhất được triển khai.*

This implementation of security in the developments is reflected in the application of the following rules:
Việc triển khai các biện pháp bảo mật trong quá trình phát triển được thể hiện thông qua việc áp dụng các quy tắc sau:

- Implementing an applicative environment, taking into account the corrective application recommendations made by the editors;
  Thiết lập môi trường ứng dụng, đồng thời có xem xét đến khuyến nghị khắc phục ứng dụng từ nhà phát triển đưa ra;
- Carrying out the rigorous control of inputs through user rights and accounts;
  Thực hiện kiểm soát nghiêm ngặt đầu vào thông qua các quyền và tài khoản của người dùng;
- Securing access on administrator functions;
  Bảo vệ quyền truy cập với các chức năng của quản trị viên;
- Applying the principle of least privilege;
  Áp dụng nguyên tắc phân phối tối thiểu;
- Prohibiting the use of passwords in the code;
  Cấm sử dụng mật khẩu trong mã nguồn;
- Implementing effective error management;
  Triển khai cơ chế quản lý lỗi hiệu quả;
- In terms of the implementation of web technologies, developments could be based on OWASP recommendations (*Open Web Application Security Project*);
  Về mặt triển khai các công nghệ web, quá trình phát triển có thể dựa theo các khuyến nghị của Dự án Bảo mật Ứng dụng Web mở (OWASP);
- Carrying out an application test, including a review of the code, making it possible to ensure that it is implemented in accordance with security requirements. The correction of potential anomalies detected during the code review are the responsibility of the Service Provider;
  Tiến hành kiểm thử ứng dụng, bao gồm rà soát mã nguồn để đảm bảo rằng quá trình triển khai tuân thủ các yêu cầu về bảo mật. Việc khắc phục các lỗi tiềm ẩn trong quá trình rà soát mã nguồn là trách nhiệm của Nhà Cung Cấp;
- Verifying the developers' abilities to make sure that the code produced does not contain malicious or back-door code;
  Kiểm tra năng lực của các lập trình viên nhằm đảm bảo mã nguồn được tạo lập không có chứa các mã độc hại hay lỗ hổng cửa hậu;
- Training developers and raising their awareness of the security rules and good practice relating to the code they are developing;
  Đào tạo và nâng cao nhận thức cho các lập trình viên về các quy tắc bảo mật và thực tiễn tốt liên quan mã nguồn mà họ đang phát triển;
- Monitoring the languages used in the developments. The security mechanisms introduced must

develop according to state of the art: the discovery of faults in an algorithm or a protocol, software or hardware implementation, or even the development of cryptanalysis techniques and attack by brute force must be taken into account.
Theo dõi các ngôn ngữ lập trình được sử dụng trong quá trình phát triển. Các cơ chế bảo mật được áp dụng phải liên tục cập nhật theo các kỹ thuật công nghệ tiên tiến: bao gồm phát hiện lỗ hổng trong các thuật toán hoặc giao thức, hoặc triển khai phần cứng hoặc phần mềm, hoặc thậm chí sự phát triển của các kỹ thuật phân tích mật mã và tấn công bằng phương pháp vét cạn đều phải được xem xét và tính toán.

7.5 ACCESS TO THE ALTEN GROUP'S IS
TRUY CẬP HỆ THỐNG PHÁT TRIỂN PHẦN MỀM CỦA TẬP ĐOÀN ALTEN

ACC1: The Service Provider undertakes to respect the general conditions for using the equipment loaned to him for the execution of Services.
ACC1: *Nhà Cung Cấp cam kết tuân thủ các điều kiện chung khi sử dụng các thiết bị được ALTEN cho mượn để thực hiện Dịch Vụ.*

ACC2: The Service Provider undertakes to respect the rules of good practice defined by the ALTEN Group and its COSI.
ACC2*: Nhà Cung Cấp cam kết tuân thủ về các quy tắc về thông lệ tốt do Tập đoàn ALTEN và Ban vận hành an toàn thông tin của Tập đoàn phê duyệt quy định.*

ACC3: In the event of an incident on an ALTEN Group workstation used by the Service Provider, the latter undertakes to respect the current procedures in place and contact the ALTEN Group teams (GALI Service Desk or IS Management).
ACC3*: Trong trường hợp xảy ra sự cố với máy trạm của Tập đoàn ALTEN mà được sử dụng bởi Nhà Cung Cấp, Nhà Cung Cấp cam kết tuân thủ các quy trình hiện hành và liên hệ với bộ phận liên quan của Tập đoàn ALTEN (Bộ phận Dịch vụ GALI hoặc Bộ phận Quản lý hệ thống thông tin).*

ACC4: All documents provided by the ALTEN Group or produced by the Service provider as part of the Services must be classified according to the degree of confidentiality (C0 to C3) and stored in the ALTEN Group's document infrastructures (shared servers or SharePoint) and not on the workstation or any external data device (USB stick, CD, DVD, external hard-drive).
ACC4*: Tất cả các tài liệu do Tập đoàn ALTEN cung cấp hoặc được tạo ra bởi Nhà Cung Cấp trong khuôn khổ Dịch Vụ phải được phân loại theo mức độ bảo mật (từ C0 đến C3) và lưu trữ trong hạ tầng dữ liệu của Tập đoàn ALTEN (máy chủ chia sẻ hoặc SharePoint) và nghiêm cấm lưu trữ các tài liệu này trên các máy trạm hoặc bất kỳ thiết bị lưu trữ dữ liệu nào (USB, CD, DVD, ổ cứng ngoài).*

7.6 LOGICAL MEANS OF ACCESS TO THE ALTEN GROUP'S IS
PHƯƠNG THỨC TRUY CẬP HỆ THỐNG THÔNG TIN CỦA TẬP ĐOÀN ALTEN THEO CÁCH TIẾP CẬN LOGIC

LMA1: Each member of the Service Provider personnel who accesses the ALTEN Group's IS has an individual account. This must be a nominative account and must only be use by this person as part of the Service being carried out.
LMA1*: Mỗi nhân sự của Nhà Cung Cấp khi truy cập vào hệ thống thông tin của Tập đoàn ALTEN phải sử dụng tài khoản cá nhân riêng biệt. Tài khoản này phải là tài khoản định danh và phải được sử dụng bởi chính người đó trong khuôn khổ Dịch Vụ đang được thực hiện.*

LMA2: Generic accounts may be used on the condition that the user can be identified.
LMA1*: Tài khoản chung có thể được sử dụng với điều kiện có thể định danh được người dùng.*

LMA3: If necessary, the Service Provider must be able to reveal the identity of the person who has used an account at a given time to the ALTEN Group.
LMA3*: Khi cần thiết, Nhà Cung Cấp dịch vụ phải có khả năng cung cấp danh tính của người đã sử dụng tài khoản tại một thời điểm nhất định cho Tập đoàn ALTEN.*

LMA4: User passwords must be changed at least once every three (3) months and must meet the ALTEN Group security requirements defined in this document.
LMA4*: Mật khẩu người dùng phải được thay đổi ít nhất ba (3) tháng một lần và phải đảm bảo đáp ứng theo những yêu cầu bảo mật của Tập đoàn ALTEN được quy định trong văn bản này.*

LMA5: The passwords for accounts used by automated applications and processes must be changed at least every three (3) months. Only the Service Provider should be able to access and modify them.
LMA5*: Mật khẩu cho các tài khoản được sử dụng bởi ứng dụng và quy trình tự động cũng phải được thay đổi tối thiểu ba (3) tháng một lần. Chỉ có Nhà Cung Cấp mới được phép truy cập và thay đổi các mật khẩu này.*

LMA6: Passwords must consist of at least eight (8) characters, combining at least three (3) out of the following four (4) factors: upper-case letters, lower-case letters, numbers and special or accented characters.
LMA6*: Mật khẩu phải có độ dài tối thiểu tám (8) ký tự, và kết hợp ít nhất ba (3) trong bốn (4) yếu tố sau: chữ in hoa, chữ thường, chữ số và ký tự đặc biệt hoặc ký tự có dấu.*

LMA7: Password strength is monitored so that they cannot be guessed, meaning that they are not derived from the user's login, his surname, first name, a date, a common word, a first name of proper noun from the French or English language, or the language of the country where the Service Provider's premises is based.
LMA7*: Độ mạnh của mật khẩu phải được kiểm soát nhằm tránh khả năng bị đoán ra, nghĩa là mật khẩu không được phép dựa trên thông tin như tên đăng nhập, họ, tên, ngày tháng, từ thông dụng, tên riêng hoặc danh từ riêng bằng tiếng Pháp, hoặc tiếng Anh, hoặc bất cứ ngôn ngữ nào nơi quốc gia của Nhà Cung Cấp đặt trụ sở.*

LMA8: Access to secret information enabling users to be authenticated must only be given to the administrators of this data, and their access must be tracked. The reasons for accessing this data must be analysed regularly.
LMA8*: Việc truy cập vào các thông tin mật để xác thực người dùng chỉ được cấp cho các quản trị viên của dữ liệu này, và mọi truy cập của phải được ghi lại. Các lý do truy cập dữ liệu này cần được phân tích thường xuyên.*

LMA9: Authentication methods include protection against attempted or mistaken attacks on authentication secrets.
LMA7*: Các phương thức xác thực phải có cơ chế bảo vệ chống lại các cuộc tấn công có chủ đích hoặc do sai sót nhằm vào thông tin xác thực bí mật.*

7.7 TRACEABILITY OF ACTIONS
KHẢ NĂNG TRUY VẾT HÀNH ĐỘNG

LOG1: It is the Service Provider's responsibility to ensure that access and event logs are active on all of the equipment for which he is responsible. A trace backup policy must exist. Ideally, these traces must be exported and centralised. The ALTEN Group may request an extract of these traces, in the event of an incident or for resource monitoring purposes.
LOG1: Nhà Cung Cấp có trách nhiệm đảm bảo rằng các nhật ký truy cập và sự kiện được kích hoạt trên tất cả các thiết bị mà họ chịu trách nhiệm. Chính sách sao lưu dấu vết phải được thiết lập. Lý tưởng nhất là các dấu vết này phải được xuất ra và tập trung hóa. Tập đoàn ALTEN có thể yêu cầu trích xuất những dữ liệu này trong trường hợp có sự cố hoặc nhằm mục đích giám sát tài nguyên.

LOG2: The Service Provider must store the connection traces on his systems for six (6) months, unless this is known to breach applicable legal requirements.
LOG2*: Nhà Cung Cấp phải lưu trữ dấu vết kết nối trên hệ thống của mình trong vòng sáu (6) tháng, trừ khi việc này được xác định là vi phạm các quy định pháp luật hiện hành.*

LOG3: Traces must be attributable to a member of the Service Provider's personnel. They are time-stamped according the Service provider's time reference point.
***LOG3**: Các dấu vết phải được quy cho một nhân viên của Nhà Cung Cấp là người chịu trách nhiệm. Các dấu vết này phải được đánh dấu thời gian theo mốc thời gian tham chiếu của Nhà Cung Cấp.*

LOG4: The minimum information to be collected and stored is:
***LOG4**: Thông tin tối thiểu cần được thu thập và lưu trữ bao gồm:*

- Connection and disconnection to the equipment and applications of the services concerned;
  Kết nối và đăng xuất khỏi thiết bị và ứng dụng liên quan đến dịch vụ;
- Consultation of information related to the private life of our clients and employees;
  Tham khảo thông tin liên quan đến đời sống cá nhân của khách hàng và nhân viên của chúng tôi;
- Internet usage information (access to websites);
  Thông tin sử dụng Internet (truy cập các trang web);
- Read-only and write-access to files and folders classified "C2 - RESTRICTED" or "C3 - STRATEGIC".
  Quyền chỉ đọc và ghi vào các tệp và thư mục được phân loại "C2 – HẠN CHẾ" hoặc "C3 – CHIẾN LƯỢC".

LOG5: Access to traces must be limited technically to guarantee integrity.
***LOG5**: Quyền truy cập các bản ghi phải được giới hạn nghiêm ngặt về mặt kỹ thuật để đảm bảo tính toàn vẹn.*

LOG6: The technology architecture established for Service Providers guarantees data integrity.
***LOG6:** Kiến trúc công nghệ được triển khai cho Nhà Cung Cấp nhằm đảm bảo tính toàn vẹn của dữ liệu.*

7.8 HOSTING AND MANAGED SERVICES
DỊCH VỤ LƯU TRỮ VÀ QUẢN LÝ

HOS1: The geographic location of the Service Provider's premises hosting IT resources involved in the ALTEN Group's IS production activities must not be exposed to natural, social or industrial risks. However, if the premises are located in an area presenting risks, the Service Provider must declare how these risks are taken into account to ensure continuity of service.
***HOS1**: Vị trí địa lý của cơ sở nơi Nhà Cung Cấp sử dụng để lưu trữ các tài nguyên công nghệ thông tin (IT) phục vụ cho hoạt động sản xuất hệ thống thông tin của Tập đoàn ALTEN, phải không bị ảnh hưởng bởi các nguy cơ rủi ro tự nhiên, xã hội hoặc công nghiệp. Tuy nhiên, nếu cơ sở đặt tại khu vực có tiềm ẩn rủi ro, Nhà Cung Cấp bắt buộc phải công bố các biện pháp đã áp dụng để xử lý những rủi ro đó nhằm đảm bảo tính liên tục của dịch vụ.*

HOS2: All installations contributing to the physical security of premises hosting IT resources involved in the ALTEN Group's IS production activities must comply with the laws and regulations in force in the host country.
***HOS2:** Tất cả các cơ sở vật chất góp phần vào việc đảm bảo an ninh vật lý tại cơ sở lưu trữ tài nguyên công nghệ thông tin (IT) của Tập đoàn ALTEN phải tuân thủ các quy định pháp luật tại quốc gia sở tại.*

HOS3: All of the equipment contributing to the security and continuity of operations must be subject to a preventive maintenance contract and must undergo regular control visits as provided for in French regulations.
***HOS3**: Tất cả các thiết bị góp phần vào việc đảm bảo an ninh và tính liên tục của hoạt động phải được đưa ra vào hợp đồng bảo trì, đồng thời phải được kiểm tra định kỳ theo đúng quy định pháp luật tại Pháp.*

HOS4: Fire protective installations must comply with the laws and regulations in force in the host

country. A fire policy must be formalised, meeting the needs identified in a risk analysis.
***HOS4**: Các hệ thống phòng cháy chữa cháy cần phải tuân thủ các quy định pháp luật hiện hành tại quốc gia sở tại. Chính sách phòng cháy chữa cháy cần được xây dựng bài bản, đáp ứng đầy đủ các yêu cầu đã được xác định qua phân tích rủi ro.*

HOS5: The premises must be protected against the direct and indirect effects of lightning.
***HOS5**: Các cơ sở vật chất phải được trang bị bảo bảo vệ khỏi các tác động trực tiếp và gián tiếp của sét.*

HOS6: Access to fire extinguishers must be clear and unobstructed. Appropriate signposting should make them easy to locate.
***HOS6**: Lối tiếp cận bình chữa cháy phải đảm bảo thông thoáng và không bị cản trở. Biển chỉ dẫn phù hợp cần được đặt để giúp mọi người dễ dàng định vị vị trí của các bình chữa cháy.*

HOS7: The routing of pipes should be outside of sensitive areas.
***HOS7**: Việc bố trí các đường dẫn ống nên được thực hiện bên ngoài các khu vực nhạy cảm.*

HOS8: Strategic areas must be equipped with a detection system.
***HOS8**: Các khu vực chiến lược phải được trang bị hệ thống phát hiện chuyên biệt.*

HOS9: Electrical installations must be subject to annual control and reinforced with infra-red thermography.
***HOS9**: Hệ thống điện phải được kiểm tra định kỳ hàng năm và được tăng cường bằng công nghệ nhiệt hồng ngoại.*

HOS10: Architecture implemented for the ALTEN Group platform and hosted at the Service Provider's premises will make it possible to guarantee service availability in accordance with contractual provisions.
***HOS10**: Kiến trúc nền tảng của Tập đoàn ALTEN, được triển khai và đặt tại cơ sở của Nhà Cung Cấp, sẽ đảm bảo khả năng sẵn sàng của dịch vụ theo đúng các điều khoản đã cam kết trong hợp đồng.*

8. SECURITY REQUIREMENTS RELATED TO THE PREMISES
YÊU CẦU BẢO MẬT LIÊN QUAN ĐẾN CƠ SỞ

8.1 SERVICES ON AN ALTEN GROUP SITE
DỊCH VỤ TẠI CƠ SỞ TẬP ĐOÀN ALTEN

LOC1: In the case of performing services on the ALTEN Group's premises, the Service Provider undertakes to follow the premises access rules.
***LOC1:** Trong trường hợp thực hiện dịch vụ tại cơ sở của Tập đoàn ALTEN, Nhà Cung Cấp cam kết tuân thủ các quy định về ra vào cơ sở.*

8.2 SERVICES ON A SERVICE PROVIDER'S PREMISES
DỊCH VỤ TẠI CƠ SỞ CỦA NHÀ CUNG CẤP

LOC2: In the event where Services are not executed at the ALTEN Group's premises, the Service Provider undertakes to specify the geographical location where the Services will be carried out.
***LOC2:** Trong trường hợp các dịch vụ không được thực hiện tại cơ sở của Tập đoàn ALTEN, Nhà Cung Cấp cam kết cung cấp thông tin về vị trí địa lý cụ thể nơi Dịch vụ sẽ được triển khai.*

LOC3: The Service Provider shall provide an exact list of the places in which the Services are executed and ALTEN Group's data is stored, by specifying the main sites, emergency sites, backup sites, etc.
***LOC3:** Nhà Cung Cấp phải cung cấp danh sách chính xác các cơ sở nơi Dịch vụ được thực hiện và nơi lưu trữ dữ liệu của Tập đoàn ALTEN, bao gồm cả các cơ sở chính, cơ sở khẩn cấp, cơ sở sao lưu, v.v.*

LOC4: The Service Provider shall take all of the appropriate measures to guarantee the security, integrity, confidentiality, availability and traceability of data and ALTEN Group information located at the Service Provider's premises.
LOC4: *Nhà Cung Cấp phải thực hiện tất cả các biện pháp phù hợp để đảm bảo an ninh, tính toàn vẹn, bảo mật, tính khả dụng và khả năng truy xuất của dữ liệu và thông tin của Tập đoàn ALTEN được lưu trữ tại cơ sở của mình.*

LOC5: The Service Provider will immediately alert the ALTEN Group security teams (COSI-ISSC) in the event of theft, disclosure or compromise of means of access, data and/or information, or for any physical and software security anomaly concerning the means of access and/or security incidents.
LOC5: *Nhà Cung cấp phải ngay lập tức thông báo cho nhóm phụ trách an ninh của Tập đoàn ALTEN (COSI – ISSC) trong trường hợp xảy ra mất cắp, rò rỉ hoặc xâm phạm các phương tiện truy cập, dữ liệu và/hoặc thông tin, hoặc bất kỳ sự cố nào liên quan đến an ninh vật lý hoặc phần mềm liên quan đến các phương tiện truy cập và/hoặc sự cố an ninh.*

LOC6: The Service Provider must ensure that security measures meet the security requirements of the ALTEN Group, and in particular:
LOC6: *Nhà cung cấp phải đảm bảo rằng các biện pháp bảo mật đều phải đáp ứng các yêu cầu về bảo mật của Tập đoàn ALTEN, và cụ thể như sau:*

- Prevent any unauthorised physical access, and any damage or intrusion to the Service Provider's premises and that of its sub-contractors containing ALTEN Group information;
  Ngăn chặn bất kỳ sự truy cập vật lý trái phép nào, cũng như bất kỳ tổn hại hoặc xâm nhập nào vào cơ sở của Nhà Cung Cấp và các nhà thầu phụ của họ có chứa thông tin của Tập đoàn ALTEN;
- Prevent the loss, damage and theft of information transmitted by the ALTEN Group;
  Ngăn chặn về việc mất mát, hư hại và trộm cắp thông tin được Tập đoàn ALTEN truyền tải;
- Trace all access and attempted illegal intrusions to the Service Provider's premises.
  Truy vết tất cả các lượt truy cập và nô lực xâm hại bất hợp pháp vào cơ sở của Nhà Cung Cấp.

LOC7: The Service Provider must ensure that physical access is limited to the strict operational needs of personnel present in the Service Provider's premises.
LOC7*: Nhà Cung Cấp phải đảm bảo rằng quyền truy cập vật lý được giới hạn theo nhu cầu hoạt động của nhân sự làm việc tại cơ sở của Nhà Cung Cấp.*

LOC8: The Service Provider must ensure that the means of supervision and protection against intrusion make it possible to physically identify the persons who have had access to the Service Provider's premises.
LOC8*: Nhà Cung Cấp phải đảm bảo rằng các phương tiện giám sát và bảo vệ chống xâm nhập cho phép nhận diện chính xác những người đã truy cập vào cơ sở của Nhà Cung Cấp.*

LOC9: The technical infrastructure of the buildings (distribution of energy and fluids, heating/air conditioning of the premises) must be redundant.
LOC9*: Hệ thống hạ tầng kỹ thuật của các tòa nhà (phân phối năng lượng và chất lỏng, hệ thống sưởi/điều hòa không khí tại cơ sở) phải có khả năng dự phòng.*

LOC10: The security equipment (fire, intrusion, video surveillance...) at the Service Provider's premises must have a backup power supply.
LOC10: *Thiết bị an ninh (bao gồm: báo cháy, chống đột nhập, camera giám sát…) tại cơ sở của Nhà Cung Cấp phải có nguồn điện dự phòng.*

LOC11: The Service Provider must have an up-to-date security register, containing the compliance certificates, records of regulatory visits and the report of the corrective measures carried out, which must identify the persons who have carried out these actions and the date.
LOC11*: Nhà Cung Cấp phải có sổ ghi chép an ninh được cập nhật đầy đủ, bao gồm các giấy chứng nhận tuân thủ, biên bản kiểm tra theo quy định và báo cáo về các biện pháp khắc phục đã được thực*

hiện. Sổ tay này phải ghi rõ người đã thực hiện các hành động đó và ngày thực hiện.

LOC12: The Service Provider's personnel must be identifiable and wear something that facilitates their identification (Badge, coloured ribbon, etc.).
***LOC12**: Nhân sự của Nhà Cung Cấp phải có thể nhận dạng được và đeo vật dụng hỗ trợ nhận diện (thẻ tên, dây đeo màu, v.v).*

8.3 REMOTE SURVEILLANCE OF THE SERVICE PROVIDER'S PREMISES
GIÁM SÁT TỪ XA TẠI CÁC CƠ SỞ CỦA NHÀ CUNG CẤP

TEL1: If surveillance of the Service Provider's premises is entrusted to a remote surveillance company, its on-site intervention periods must not exceed 30 minutes. The alarms transmitted must vary depending on the events, as a minimum:
***TEL 1:** Trường hợp việc giám sát tại các cơ sở của Nhà Cung Cấp được giao cho một công ty giám sát từ xa, thời gian can thiệp tại chỗ của công ty đó không được vượt quá 30 phút. Hệ thống cảnh báo phải được thiết lập để phân loại rõ ràng từng tình huống cụ thể, và tối thiểu bao gồm các loại cảnh báo như dưới đây:*

- Fire;
  Cảnh báo cháy nổ;
- Intrusion;
  Cảnh báo xâm nhập trái phép;
- Water damage if liquid is detected;
  Cảnh báo rò rỉ nước khi có phát hiện chất lỏng;
- Other alarms essential for the centralised technical management of the building.
  Các cảnh báo khác thiết yếu phục vụ công tác quản lý kỹ thuật tập trung của tòa nhà.

9. OTHER SECURITY REQUIREMENTS
CÁC YÊU CẦU KỸ THUẬT KHÁC

9.1 OVERALL MEASURES
CÁC BIỆN PHÁP TỔNG THỂ

ORG1: The Service Provider must be able to provide a formalised security policy, the scope of which covers the risks of service continuity and malicious intent to which it is exposed in connection with the Services.
***ORG1**: Nhà Cung Cấp phải có khả năng cung cấp chính sách an ninh được xây dựng thành văn bản, với phạm vi bao phủ các rủi ro liên quan đến liên tục của dịch vụ và các hành vi gây hại mà đơn vị có thể đối mặt trong quá trình cung cấp Dịch vụ.*

ORG2: The Service Provider's organisation must have at least one Security Officer for all of the areas contributing to the proper execution of the Services. The latter will be the contact point for the ALTEN Group's security teams (CISO-ISSC) in the event of an incident.
***ORG2**: Tổ chức của Nhà Cung Cấp phải có ít nhất một Chuyên viên phụ trách An ninh, chịu trách nhiệm cho tất cả các lĩnh vực liên quan đến đảm bảo Dịch vụ được thực hiện một cách có hiệu quả. Nhân sự này cũng sẽ là đầu mối liên hệ chính với bộ phận An ninh của Tập đoàn ALTEN (CISO – ISSC) trong trường hợp xảy ra sự cố.*

ORG3: The Service Provider must provide the contact information for its Security Officer and inform the ALTEN Group of any changes.
***ORG3:** Nhà Cung Cấp phải cung cấp đầy đủ các thông tin liên hệ của Chuyên viên phụ trách An ninh và thông báo cho Tập đoàn ALTEN nếu có bất kỳ thay đổi nào.*

ORG4: All Service Provider employees involved in the execution of Services must respect all of the procedures and security regulations applicable as part of the Services.

***ORG4**: Tất cả nhân sự của Nhà Cung Cấp tham gia vào quá trình thực hiện Dịch vụ phải tuân thủ đầy đủ các quy trình và quy định về an ninh hiện hành áp dụng trong phạm vi cung cấp Dịch vụ.*

ORG5: The Service Provider's Security Officer is responsible for checking the security and continuity measures in place and providing a report to the ALTEN Group's security teams (CISO or ISSC).
***ORG5**: Chuyên viên phụ trách An ninh của Nhà Cung Cấp có trách nhiệm kiểm tra các biện pháp bảo mật và đảm bảo tính liên tục của các biện pháp được triển khai, đồng thời lập báo cáo cho bộ phận an ninh của Tập đoàn ALTEN (CISO – ISSC).*

9.2 PURCHASES
MUA SẮM

ACH1: The Service Provider undertakes to respect the ALTEN Group's purchasing procedures, particularly in terms of consultations, referencing, evaluation and respecting the procurement cycle.
***ACH1:** Nhà Cung Cấp cam kết tuân thủ quy trình mua sắm của Tập đoàn ALTEN, đặc biệt là các yêu cầu liên quan đến việc tham vấn, tham chiếu, đánh giá và tuân thủ quy trình mua sắm.*

9.3 SECURITY FILE OR SECURITY ASSURANCE PLAN
THƯ MỤC BẢO MẬT VÀ KẾ HOẠCH ĐẢM BẢO AN NINH

SAP1: The Service Provider must formalise a "Security File", also referred to as a "Security Assurance Plan" (SAP). It outlines all of the specific provisions that the Service Provider undertakes to implement in the execution of Services to guarantee that the ALTEN Group's security requirements are met.
***SAP1:** Nhà Cung Cấp phải cần xây dựng một "Thư mục bảo mật", còn được gọi là "Kế hoạch Đảm bảo An ninh" (SAP). Tài liệu này nêu rõ các biện pháp cụ thể mà Nhà Cung Cấp cam kết triển khai trong quá trình thực hiện Dịch vụ, nhằm đảm bảo đáp ứng đầy đủ các yêu cầu về an ninh của Tập đoàn ALTEN.*

9.4 *SERVICE LEVEL AGREEMENT*
THỎA THUẬN MỨC ĐỘ DỊCH VỤ

SLA1: A service level agreement must be formalised between the Service Provider and the ALTEN Group. This is an agreement between the Service Provider and the ALTEN Group, outlining in particular the levels of service expected (*Service Level Agreement*).
***SLA1**: Thỏa thuận mức độ dịch vụ phải được thiết lập giữa Nhà Cung Cấp và Tập đoàn ALTEN. Đây là văn bản xác nhận mức độ dịch vụ mong đợi mà hai bên – Nhà Cung Cấp và Tập đoàn ALTEN cùng thống nhất.*

9.5 AWARENESS RAISING AND TRAINING
NÂNG CAO NHẬN THỨC VÀ ĐÀO TẠO

ART01: In the situation where the Service Provider performed services on the ALTEN Group's IS, it must ensure that its employees are properly acquainted with the IS security and good practices in place within the ALTEN Group.
***ART01:** Trong trường hợp Nhà Cung Cấp thực hiện dịch vụ trên hệ thống thông tin của Tập đoàn ALTEN, đơn vị này phải đảm bảo rằng nhân viên của mình đã được trang bị đầy đủ kiến thức về an ninh hệ thống và thực tiễn tốt đang được áp dụng trong Tập đoàn ALTEN.*

ART02: The Service Provider undertakes to outline the measures that will make it possible to guarantee that its employees respect the security requirements outlined in this document and the rules of good practice communicated by the ALTEN Group.
***ART02:** Nhà Cung Cấp cam kết trình bày rõ những biện pháp nhằm bảo đảm nhân viên của mình tuân thủ đầy đủ các yêu cầu về bảo mật được nêu trong văn bản này cũng như các quy tắc thực tiễn tốt do Tập đoàn ALTEN ban hành.*

ART03: The Service Provider performing the Services on the ALTEN Group's IS undertakes to follow,

at its own expense and from the start of the Services, the ALTEN Group's IS security awareness raising module via the "ALTEN Training Centre" platform.

ART03: *Nhà Cung Cấp khi thực hiện dịch vụ Dịch vụ trên hệ thống an ninh của Tập đoàn ALTEN cam kết, ngay từ khi bắt đầu cung cấp Dịch vụ và bằng chi phí của mình, cần hoàn thành khóa học nâng cao nhận thức về an toàn hệ thống thông tin thông qua nền tảng "Trung tâm Đào tạo ALTEN".*

9.6 SUB-CONTRACTING
THẦU PHỤ

SC1: In contracts concluded with sub-contractors, the Service Provider incorporates all of the ALTEN Group's security requirements that must be respected by the sub-contractor.
SC1: *Trong các hợp đồng được ký kết với các nhà thầu phụ, Nhà Cung Cấp phải quy định đầy đủ các yêu cầu về bảo mật của Tập đoàn ALTEN mà nhà thầu phụ buộc phải tuân thủ.*

SC2: In the case of sub-contracting authorised by the ALTEN Group, the Service Provider undertakes to ensure that the sub-contractors respect the security requirements defined in this document and implements a sub-contractor evaluation process to check that the ALTEN Group's security requirements are being respected.
SC2: *Trong trường hợp việc sử dụng thầu phụ được Tập đoàn ALTEN chấp thuận, Nhà Cung Cấp cam kết đảm bảo rằng các nhà thầu phụ tuân thủ nghiêm ngặt các yêu cầu an ninh được quy định trong tài liệu này, đồng thời triển khai quy trình đánh giá nhà thầu phụ nhằm kiểm tra việc tuân thủ các yêu cầu bảo mật của Tập đoàn ALTEN.*

9.7 TREATMENT OF PERSONAL DATA
XỬ LÝ DỮ LIỆU CÁ NHÂN

CNIL1: The Service Provider undertakes that personal data will be processed in a country authorised by the European Commission and the competent national authorities responsible for information management and the treatment of personal data.
CNIL1: *Nhà Cung Cấp cam kết rằng dữ liệu cá nhân chỉ được xử lý tại các quốc gia được Ủy ban Châu Âu và quốc gia có thẩm quyền về quản lý thông tin và xử lý dữ liệu cá nhân cho phép.*

CNIL2: In the event where Services are sub-contracted with the prior approval of the ALTEN Group, the Service Provider must ensure that the treatment of personal data by its sub-contractors also meets the regulations described in the previous point. (**CNIL1)**.
CNIL2: *Trong trường hợp Dịch vụ được chuyển giao cho nhà thầu phụ với sự chấp thuận trước của Tập đoàn ALTEN, Nhà Cung Cấp phải đảm bảo rằng việc xử lý dữ liệu cá nhân bởi các nhà thầu phụ phải tuân thủ các quy định được nêu tại điểm CNIL1 ở trên.*

CNIL3: The Service Provider undertakes that personal data shall be processed and protected in compliance with recommendations of CNIL and Law no. 78-17 of 6 January 1978 on information technology, data files and civil liberties amended by Law no. 2004-801 of 6 August 2004 relating to the protection of data subjects as regards the processing of personal data.
CNIL3: *Nhà Cung Cấp cam kết rằng dữ liệu cá nhân sẽ được xử lý và bảo vệ phù hợp với khuyết nghị Ủy ban Quốc gia về Tin học và Tự do của Pháp và theo quy định của Luật số 78-17 ngày 06 tháng 01 năm 1978 tin học, tập tin dữ liệu cà quyền tự do dân sự, đã được sửa đổi bởi Luật số 2004-801 ngày 06 tháng 06 năm 2004 liên quan đến bảo vệ chủ thể dữ liệu và xử lý dữ liệu cá nhân.*

9.8 DATA PROTECTION
BẢO VỆ DỮ LIỆU

DAT1: Any information and/or data classified C1 (Internal), C2 (Restricted) or C3 (Strategic) and transferred as part of a Service must be subject to signed confidentiality agreement between the ALTEN Group and the Service Provider. The Service Provider must:
DAT 1*: Bất cứ thông tin và/hoặc dữ liệu nào được phân loại C1 (Nội bộ), C2 (Hạn chế) hoặc C3 (Chiến*

lược) và được chuyển giao trong khuôn khổ Dịch vụ, đều phải chịu sự ràng buộc thỏa thuận bảo mật đã được ký kết giữa Tập đoàn ALTEN và Nhà Cung Cấp. Nhà Cung Cấp phải:

- Make sure its employees respect this agreement;
  Đảm bảo rằng nhân sự của mình tuân thủ đầy đủ các điều khoản trong thỏa thuận bảo mật này;
- Take care not to disclose information in accordance with the terms of the agreement;
  Không tiết lộ bất cứ thông tin nào, phù hợp với các điều khoản của thỏa thuận;
- Restore the data at the end of the Services and/or destroy the data on all device containing it.
  Hoàn trả toàn bộ dữ liệu sau khi kết thúc Dịch vụ và/hoặc tiến hành hủy toàn bộ dữ liệu ra khỏi mọi thiết bị có chứa dữ liệu đó.

DAT2: All Service Provider's participating in the execution of Services must signed a personal confidentiality agreement.
DAT2: *Tất cả nhân viên của Nhà Cung Cấp tham gia vào quá trình thực hiện Dịch vụ đều phải ký thỏa thuận bảo mật thông tin.*

DAT3: The Service Provider is responsible for the confidentiality and integrity of information in its possession and undertakes to implement any means necessary to guarantee the security of ALTEN Group information.
DAT3: *Nhà Cung Cấp chịu trách nhiệm về tính bảo mật và toàn vẹn của thông tin do mình quản lý, và cam kết thực hiện mọi biện pháp cần thiết để đảm bảo tính bảo mật đối với toàn bộ thông tin của Tập đoàn ALTEN.*

All Parties receiving restricted (C2) and strategic (C3) information undertake to:
Tất cả các Bên nhận thông tin được phân loại ở mức Hạn chế (C2) và Chiến lược (C3) cam kết:

- Keep it confidential and not publish it or disclose it to third-parties;
  Giữ bí mật và không công bố hay tiết lập thông tin với bất kỳ bên thứ ba nào;
- Not use Confidential Information for any purpose other than that specified in the agreement;
  Không tiết lộ bất kỳ thông tin cho bất kỳ mục đích nào khác ngoài mục đích đã được quy định trong thỏa thuận;
- Take all necessary measures to protect the confidentiality and integrity of the information;
  Thực hiện mọi biện pháp cần thiết để bảo vệ tính bảo mật và tính toàn vẹn của thông tin;
- Restrict the communication of and access to this information to the Directors, employees, representatives, consultants and sub-contractors who need to know the information and, in this case, ensure that these persons respect the confidential nature of the information;
  Hạn chế truyền đạt và truy cập loại thông tin này cho các Giám đốc, nhân viên, đại diện, tư vấn viên và nhà thầu phụ - những người có liên quan cần phải biết các thông tin đó, và trong trường hợp đó phải đảm bảo rằng các cá nhân này phải tuân thủ nghiêm ngặt bảo mật thông tin;
- Not create any copies for third-parties.
  Không tạo bản sao cho bất kỳ bên thứ ba nào.

9.9 INCIDENTS AND ALERTS
SỰ CỐ VÀ CẢNH BÁO

INC1: The Service Provider undertakes to set up an alert procedure with the ALTEN Group's operational (Contract Manager) and security teams (CISO - ISSC), facilitating fast and effective collaboration in the event of a security incident, suspected intrusion or data compromise.
INC1*: Nhà Cung Cấp cam kết thiết lập một quy trình cảnh báo phối hợp với các bộ phận vận hành (Quản lý Hợp đồng) và bộ phận an ninh (CISO – ISSC) của Tập đoàn ALTEN, nhằm đảm bảo khả năng phối hợp nhanh chóng và hiệu quả trong trường hợp xảy ra sự cố an ninh, nghi ngờ, nghi ngờ xâm nhập trái phép hoặc rò rỉ dữ liệu.*

9.10 DELETION OF DATA AND/OR INFORMATION
XÓA DỮ LIỆU VÀ/HOẶC THÔNG TIN

DEL1: In the case where the Service Provider recovers grants, scraps, media (CD, DVD, disks, backup tapes, USB sticks, cards, etc.) containing ALTEN Group data/information during maintenance, the Service Provider undertakes to securely erase this data media and delete the data and/or information, according to the state of the art and the recommendations of the French National Information System Security Agency (ANSSI).

DEL1*: Trong trường hợp Nhà Cung Cấp thu hồi các thiết bị, linh kiện, phương tiện lưu trữ (CD, DVD, đĩa cứng, băng sao lưu, USB, thẻ, v.v) có chứa dữ liệu/thông tin của Tập đoàn ALTEN trong suốt quá trình bảo trì, Nhà Cung Cấp cam kết xóa bỏ an toàn các phương tiện lưu trữ này và loại bỏ dữ liệu/thông tin đó, phù hợp với các giải pháp công nghệ tiên tiến và theo khuyến nghị của Cơ quan An ninh Hệ thống Thông tin Quốc gia Pháp (ANSSI).*

DEL2: If the ALTEN Group trusts the Service Provider with data and/or information that may be stored on the Service Provider's devices (PC, servers, data storage media), and in the event that the Service Provider stops using these devices (change of allocation, repair, replacement, destruction), the Service Provider assures the ALTEN Group that the data and/or information stored will be classified and handled as necessary (archiving, recovery, destruction, etc.).

DEL2: *Trong trường hợp Tập đoàn ALTEN chuyển giao dữ liệu và/hoặc thông tin cho Nhà Cung Cấp và những dữ liệu này có thể được lưu trữ trên các thiết bị của Nhà Cung Cấp (máy tính, máy chủ, thiết bị lưu trữ dữ liệu), thì trong trường hợp Nhà Cung Cấp ngừng sử dụng các thiết bị nêu trên (do thay đổi mục đích sử dụng, sửa chữa, thay thế hoặc tiêu hủy), Nhà Cung Cấp cam kết với Tập đoàn ALTEN rằng mọi dữ liệu và/hoặc thông tin lưu trữ sẽ được phân loại và xử lý phù hợp (chẳng hạn như: lưu trữ, khôi phục, tiêu hủy, v.v).*

DEL3: In accordance with the ALTEN Group's policy for handling information, the Service provider must implement the procedures and tools for the deletion of data and/or information as part of the Services. For paper-based information, shredders will be use (standard DIN32757) to delete the ALTEN Group's data and/or information, or any other method that complies with current legislation.

DEL3: *Nhằm đảm bảo phù hợp với chính sách về xử lý thông tin của Tập đoàn ALTEN, Nhà Cung Cấp phải đảm bảo triển khai các quy trình và công cụ cần thiết để xóa dữ liệu và/hoặc thông tin trong phạm vi cung cấp Dịch vụ. Đối với thông tin được lưu trữ trên giấy, thì cần sử dụng máy hủy tài liệu tiêu chuẩn (theo tiêu chuẩn DIN32757) để xóa dữ liệu và/hoặc thông tin của Tập đoàn ALTEN hoặc bất kỳ phương pháp khác tuân thủ theo quy định pháp luật hiện hành.*

9.11 CONFIDENTIALITY
BẢO MẬT

ORG6: All of the documents and information exchanged between the Service Provider and the ALTEN Group are classed according to the degree of confidentiality in compliance with the framework defined below:

ORG6: *Tất cả tài liệu và thông tin trao đổi giữa Nhà Cung Cấp và Tập đoàn ALTEN đều phải được phân loại theo mức độ bảo mật và dựa trên khung phân loại được định nghĩa như dưới đây:*

- C0 - "PUBLIC" Information: Basic security requirements, for public data, documents or information having a low impact in the event of a security incident. Data or information intended to be published;
  C0 – Thông tin "CÔNG KHAI": Áp dụng các yêu cầu bảo mật cơ bản, dành cho dữ liệu, tài liệu hoặc thông tin công khai có mức độ ảnh hưởng thấp trong trường hợp xảy ra sự cố an ninh. Đây là những dữ liệu hoặc thông tin được phép công bố rộng rãi;

- C1 - "INTERNAL" Information: Basic security requirements, for data, documents or information for internal use having a moderate impact in the event of a security incident;
  C1 – Thông tin "Nội bộ": Áp dụng các yêu cầu bảo mật cơ bản, dành cho dữ liệu hoặc thông tin sử dụng nội bộ, có mức độ ảnh hưởng trung bình trong trường hợp xảy ra sự cố an ninh;

- C2 - "RESTRICTED" Information: Higher level of security requirements requiring the

implementation of controls and protective measures for data, documents or information having a high impact on business activities in the event of a security incident;
C2 – Thông tin "HẠN CHẾ": Yêu cầu mức độ bảo mật cao hơn, đòi hỏi cần phải triển khai các biện pháp kiểm soát và bảo vệ đối với dữ liệu, tài liệu hoặc thông tin có thể gây ảnh hưởng nghiêm trọng trong trường hợp xảy ra sự cố an ninh;

- C3 - "STRATEGIC" Information: High level security requirements, requiring the highest level of control and protective measures for data, documents or information having a critical impact on business activities in the event of a security incident.
C3 – Thông tin "CHIẾN LƯỢC": Đây là loại thông tin có yêu cầu bảo mật ở mức cao nhất, đòi hỏi các biện pháp kiểm soát và bảo vệ nghiêm ngặt nhất đối với dữ liệu, tài liệu hoặc thông tin có thể ảnh hưởng nghiêm trọng đến hoạt động kinh doanh nếu xảy ra sự cố an ninh

If data, documents or information such as IS security policies must be distributed to a Service Provider, a distribution list, at the top of the document, must state all recipients external to the ALTEN Group.
Trong trường hợp các dữ liệu, tài liệu hoặc chẳng hạn như Chính sách về bảo mật hệ thống thông tin cần được chia sẻ với Nhà Cung Cấp thì phải có danh sách phân phối ở đầu tài liệu, trong đó liệt kê rõ tất cả các bên nhận bên ngoài Tập đoàn ALTEN.

All intended recipients shall undertake to respect the confidentiality and integrity of the data, documents or information exchanged.
Tất cả các bên nhận dự kiến đều phải cam kết tôn trọng tính bảo mật và toàn vẹn của dữ liệu, tài liệu hoặc thông tin được trao đổi.

9.12 BUSINESS CONTINUITY
TÍNH LIÊN TỤC CỦA HOẠT ĐỘNG KINH DOANH

9.12.1 Continuity of Standard Activities
Duy trì các hoạt động tiêu chuẩn

BCP1: Escalations in the event of disasters must be defined, controlled and shared between the Service Provider and the ALTEN Group. A contact person must be identified to report the occurrence of a crisis.
BCP1: *Quy trình báo cáo và xử lý trong trường hợp xảy ra thảm họa phải được quy định rõ ràng, kiểm soát chặt chẽ và được chia sẻ giữa Nhà Cung Cấp và Tập đoàn ALTEN. Một đầu mối liên lạc cụ thể cần được chỉ định để báo cáo khi có khủng hoảng xảy ra.*

BCP2: In the Security File (SAP), the Service provider shall outline the standard business continuity provisions that exist and apply to the scope of the contract. Measures (physical and organisational) must be put in place to meet the continuity requirements expressed by the ALTEN Group.
BCP2: *Trong Thư mục Bảo mật (SAP), Nhà Cung Cấp phải trình bày rõ ràng các biện pháp bảo đảm tính liên tục trong hoạt động kinh doanh hiện tại và áp dụng trong phạm vi của hợp đồng. Đồng thời, phải thiết lập các biện pháp (về mặt vật lý và tổ chức) nhằm đáp ứng yêu cầu về tính liên tục do Tập đoàn ALTEN đưa ra.*

BCP3: All of the systems must provide for the regular outsourcing of its data, so that it can be recovered in the case of a disaster.
BCP3: *Toàn bộ hệ thống cần phải đảm bảo cơ chế sao lưu dữ liệu thường xuyên ra bên ngoài nhằm mục đích khôi phục trong trường hợp xảy ra sự cố.*

9.12.2 Continuity of activities hosted by the Service Provider
Đảm bảo tính liên tục của các hoạt động lưu trữ bởi Nhà Cung Cấp

BCP4: Measures (physical and organisational) must be put in place to meet the continuity requirements expressed by the ALTEN Group. These measures will be outlined in the Security File (SAP).
BCP4: *Các biện pháp (về mặt vật lý và tổ chức) cần phải được triển khai nhằm đáp ứng yêu cầu về*

tính liên tục do Tập đoàn ALTEN đề ra. Những biện pháp này sẽ được đề cập chi tiết Thư mục bảo mật (SAP).

BCP5: Data outsourced to assist in the event of disaster must be verified as part of regular controls.
***BCP5:** Để đảm bảo khả năng khôi phục dữ liệu trong trường hợp xảy ra sự cố, dữ liệu sao lưu bên ngoài cần phải được kiểm tra định kỳ như một phần trong quy trình kiểm soát thường xuyên.*

BCP6: All of the documentation related to business continuity must be reviewed regularly or during key events to guarantee that its content is up-to-date and applicable in the event of disaster.
***BCP6:** Mọi tài liệu liên quan đến duy trì hoạt động kinh doanh cần phải được kiểm tra định kỳ hoặc khi có sự kiện quan trọng, nhằm đảm bảo nội dung luôn được cập nhật và có thể áp dụng trong trường hợp xảy ra sự cố.*

BCP7: Persons involved in recovery plans must be regularly sensitised and trained in order to maintain their level of knowledge and ensure the effectiveness of continuity plans.
***BCP7:** Những cá nhân tham gia vào các kế hoạch khắc phục cần được nâng cao nhận thức vào đào tạo định kỳ để nhằm duy trì kiến thức chuyên môn và đảm bảo hiệu quả về tính liên tục đối với các kế hoạch triển khai.*

BCP8: Emergency drills must be carried out regularly and the report sent to the appropriate ALTEN Group Manager.
***BCP8:** Các buổi diễn tập khẩn cấp phải được tổ chức thường xuyên và báo cáo kết quả phải được gửi tới Cấp Quản lý phụ trách theo đúng thẩm quyền của Tập đoàn ALTEN.*

9.13 RETURN OF THE PROJECT
HOÀN TRẢ DỰ ÁN

RET1: The Service Provider shall provide the necessary assistance during the migration period to facilitate the transfer of hardware and software security means, and the resumption of the operation by the ALTEN Group, or by another Service Provider.
***RET1**: Nhà Cung Cấp có trách nhiệm hỗ trợ cần thiết trong giai đoạn chuyển đổi để tạo điều kiện thuận lợi cho việc chuyển giao các phương tiện bảo mật phần cứng và phần mềm, và việc tiếp quản hoạt đoạt bởi Tập đoàn ALTEN hoặc Nhà Cung Cấp khác.*

RET2: During the transfer, the Service Provider undertakes to guarantee the security of the data and applications entrusted to him, in accordance with his obligations.
***RET2**: Trong suốt quá trình chuyển giao, Nhà Cung Cấp cần đảm bảo tính bảo mật của dữ liệu và các ứng dụng được giao phó, phù hợp với các nghĩa vụ của mình.*

RET3: In the event of stoppage of the Services, all of the equipment, software and documents entrusted to the Service Provider must be returned. The non-restitution of all or part of this property will be considered and treated as a loss.
***RET3**: Trong trường hợp dừng sử dụng Dịch vụ, toàn các thiết bị, phần mềm và tài liệu đã được giao cho Nhà Cung Cấp phải được hoàn trả lại. Việc không hoàn trả toàn bộ hoặc một phần các tài sản sẽ bị coi là tổn thất và sẽ được xử lý như một sự cố mất mát tài sản.*

RET4: Partial restitution may be requested by the ALTEN Group, in the event of stoppage of a part of the Services before the end of the contract. In this case, the Service Provider will be informed at least one month before the end of the Service.
***RET4**: Tập đoàn ALTEN có thể yêu cầu hoàn trả một phần trong trường hợp việc ngừng sử dụng một phần Dịch vụ trước thời hạn kết thúc hợp đồng. Trong trường hợp này, Nhà Cung Cấp sẽ được thông báo ít nhất một tháng trước thời điểm chấm dứt Dịch vụ.*

RET5: At the end of the contract, the Service Provider must transfer the information about the operational and technical context of the applications set to the future Service Provider team, as well as

the follow-up aspects of the project.
***RET5**: Tại thời điểm kết thúc hợp đồng, Nhà Cung Cấp phải chuyển giao thông tin liên quan đến bối cảnh vận hành và kỹ thuật của các ứng dụng cho đội ngũ của Nhà Cung Cấp kế nhiệm, cũng như các khía cạnh liên quan đến việc theo dõi dự án.*

9.14 AUDIT
KIỂM TRA

AUD1: The Service Provider shall authorise the ALTEN Group to conduct security audits to verify that the Service Provider is respecting his obligation to maintain the level of security required by the ALTEN Group, particularly the proper application of the SAP. The Service Provider will be given at least thirty (30) working days notice of an audit.
***AUD1**: Nhà Cung Cấp cho phép Tập đoàn ALTEN tiến hành các cuộc kiểm tra an ninh nhằm đánh giá việc tuân thủ các nghĩa vụ liên quan đến duy trì mức độ bảo mật theo yêu cầu của Tập đoàn ALTEN, đặc biệt là việc áp dụng đầy đủ Kế hoạch Đảm bảo An ninh đối với Nhà Cung Cấp. Tập đoàn ALTEN sẽ thông báo cho Nhà Cung Cấp trước ít nhất ba mươi (30) ngày làm việc trước khi tiến hành kiểm tra.*

AUD2: The Service Provider shall authorise the ALTEN Group to conduct security audits to verify the protection of ALTEN Group data, without notice. The frequency of these impromptu audits must be established with the Service Provider when signing the contract.

***AUD2**: Nhà Cung Cấp cho phép Tập đoàn ALTEN tiến hành các cuộc kiểm tra an ninh mà không cần thông báo trước nhằm xác minh việc bảo vệ dữ liệu của Tập đoàn ALTEN. Tần suất thực hiện các cuộc kiểm tra này phải được thống nhất tại thời điểm ký kết hợp đồng với Nhà Cung Cấp.*

AUD3: Following the audit, the Service Provider must submit an action plan to the ALTEN Group for approval, fifteen (15) days after the delivery of the audit report.
***AUD3**: Sau khi cuộc kiểm tra được thực hiện, Nhà Cung Cấp có trách nhiệm gửi một kế hoạch hành động cho Tập đoàn ALTEN xem xét và phê duyệt, trong vòng mười lăm (15) ngày sau khi báo cáo kiểm tra được bàn giao.*

AUD4: Any discrepancies established in the audit report and, more generally, any non-compliance with the ALTEN Group's security requirements, must be regularised within a period agreed upon by both parties. Delays may be subject to penalties.
***AUD4**: Bất kỳ sai lệch nào được nêu trong báo cáo kiểm tra, và nói chung là bất kỳ hành vi không tuân thủ nào đối với các yêu cầu bảo mật của Tập đoàn ALTEN, phải được khắc phục trong thời hạn hai bên thỏa thuận. Trường hợp chậm trễ có thể dẫn đến việc áp dụng chế tài.*

AUD5: The Service Provider must give the ALTEN Group the right to access all of the elements related to the audit.
***AUD5**: Nhà Cung Cấp phải cung cấp cho Tập đoàn ALTEN quyền truy cập vào tất cả các tài liệu, thông tin và yếu tố liên quan đến hoạt động kiểm tra.*

AUD6: The Service Provider shall authorize the ALTEN Group to test or have tested the secure measures implemented by the Service Provider.
***AUD6**: Nhà Cung Cấp cho phép Tập đoàn ALTEN tiến hành kiểm tra hoặc cho phép kiểm tra các biện pháp bảo mật đã được Nhà Cung Cấp triển khai.*

AUD7: The vulnerabilities identified during security tests must be addressed through suitable measures based on an action plan approved by the ALTEN Group and the security methods file will be updated accordingly.
***AUD7**: Các lỗ hổng đã được xác định trong quá trình bảo mật phải được xử lý bằng các biện pháp phù hợp dựa trên kế hoạch hành động được Tập đoàn ALTEN phê duyệt và thư mục phương thức bảo mật sẽ được cập nhật tương ứng.*

10. ACCEPTANCE OF THE ALTEN GROUP'S SECURITY REQUIREMENTS/CHẤP THUẬN CÁC YÊU CẦU BẢO MẬT CỦA TẬP ĐOÀN ALTEN

This document is an integral part of the General Terms and Conditions of Purchasing and applies to all ALTEN Group Service Providers.

Tài liệu này là một phần không thể tách rời của Điều Khoản và Điều Kiện Chung được áp dụng với tất cả Nhà Cung Cấp của Tập đoàn ALTEN.

The suppliers acknowledge and agree that the commencement of any commercial relationship with the ALTEN Group automatically constitutes confirmation that they:

Việc Nhà Cung Cấp xác nhận đã hiểu rõ và nhận thức rằng việc bắt đầu bất kỳ mối quan hệ thương mại nào với Tập đoàn ALTEN được hiểu cấu thành sự xác nhận của Nhà Cung Cấp:

- *Have taken note of the* ALTEN Group's Security Requirements*;*
  Đã đọc và nắm rõ các Yêu Cầu Bảo Mật của Tập đoàn ALTEN;
- Commit to strictly complying with all of its provisions, and acknowledge that any breach may result in the termination of commercial relations;
  Cam kết tuân thủ nghiêm ngặt toàn bộ quy định trong Yêu Cầu Bảo Mật này và thừa nhận rằng mọi vi phạm có thể dẫn đến việc chấm dứt quan hệ thương mại;
- Commit to ensuring that all of its provisions are strictly complied with by any subcontractors and suppliers they may use.
  Cam kết đảm bảo tất cả các quy định này cũng được tuân thủ nghiêm ngặt bởi bất cứ nhà thầu phụ và nhà cung cấp nào mà Nhà Cung Cấp sử dụng.