Information Security Policy

Introduction

The goal of the Information Security Policy is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic "need-to-know" principle.
- Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

EBI has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.
This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to EBI by its stakeholders, partners, customers and other third-parties.

Purpose

The purpose of the Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to EBI, its business partners, and its stakeholders.

Audience

The Information Security Policy applies equally to any individual, entity, or process that interacts with any EBI Information Resource.

Responsibilities

1) Distributor will adhere to EBI information security requirements set out in this Policy for the storing, processing, transmitting, and handling of EBI Restricted Information.

2) Distributor will establish and maintain administrative, technical, and physical safeguards that are consistent with industry standards and designed to prevent Security Incidents. This includes: (i) protecting the confidentiality, integrity, and availability of the Distributor Systems; (ii) implementing technical controls to guard against anticipated threats or hazards to Distributor Systems; and (iii) implementing controls to prevent unauthorized physical access, remote access, damage to, or disruption of, the Distributor Systems.

3) Distributor, along with any subcontractors, and/or Affiliates of Distributor who process, transmit or store EBI Restricted Information, shall handle all EBI Restricted Information according to industry best practices including but not limited to:
    a. Use only operating systems and applications that are sufficiently hardened to prevent system misuse and tampering.
    b. Use industry standard encryption and key management methods.

c. Encrypt all EBI Restricted Information while in-transit and at-rest, regardless of transport mode or media type; provided that all parties shall agree in advance on a method of exchange in case of a need to exchange encrypted information.
d. Routinely update, patch, and protect all software and systems developed, maintained, and/or operated by Distributor in relation to its access to and use of the Services.
e. Establish and maintain least privileged access controls for all Distributor Systems that process, transmit, or store EBI Restricted Information. Access controls must include account provisioning, de-provisioning, authentication, authorization, and accountability controls.
f. Log, monitor, and protect all user activities, actions, exceptions, and information security events on all Distributor Systems that process, transmit, or store EBI Restricted Information. Distributor shall provide copies of any logs to EBI upon request.
g. Use automated or programmatic means to deploy, maintain, update, configure, patch, fix, log, and monitor the systems and connections used in relation to the Services.
h. Use multi-factor authentication consistent with current industry standards to access EBI Restricted Information or any Distributor Systems that transmit, process or store EBI Restricted Information.
i. Implement controls that are consistent with industry standards to ensure that Distributor Systems used to process, transmit, or store EBI Restricted Information are protected against viruses and malware.
j. Implement and use solutions consistent with industry standards for actively managed and defended endpoint protections, external network ingress and egress connectivity (Internet, extranet, VPN), email filtering, banners and other protections.
k. Limit data that is transmitted, processed, or stored to only what is necessary to utilize the Services from EBI in the manner set forth in contractual documentation entered into between EBI and Distributor.
l. Maintain proper segmentation of EBI Restricted Information in Distributor Systems that process, transmit or store EBI Restricted Information.
m. Upon request by EBI, Distributor shall provide all EBI Restricted Information in the Distributor Systems.
n. Establish and maintain a Vulnerability Management Program for all Distributor Systems processing, transmitting, or storing EBI Restricted Information.
o. Document system environment and provide EBI with any data-flow diagrams or system architecture diagrams used in relation to its access to and use of the Services that process, transmit, or store EBI Restricted Information.
p. Maintain a formal change management process for Distributor Systems that process, transmit, or store EBI Restricted Information.

All Employees, Contractors, and Other Third-Party Personnel

- Use EBI Information Resources in compliance with all EBI information security requirements.
- Seek guidance from the EBI Security Engineering team for questions or issues related to information security.

Information Security Representations and Warranties

- Distributor represents and warrants as follows on behalf of itself, its Affiliates and any sub-distributors:
    - Distributor shall ensure remote access to any Distributor Systems is not allowed from locations of Nigeria, Russia, China, North Korea, Iran, or Israel.
    - Distributor shall provide industry standard privacy and information security training to their employees and subcontractors.
    - Distributor will not introduce any disabling mechanism or device, hidden program, time-out mechanism, virus or other computer programming routines that could or does damage, disrupt, provide unauthorized access to, detrimentally interfere with, surreptitiously intercept, or expropriate any system, used for the provision of, or receipt of, the Services.
    - Any software, managed service, or other IPR used by Distributor in connection with its use of the Services does not infringe, misappropriate, or otherwise violate any intellectual property rights of any third party and does not violate the laws or regulations of Switzerland, the European Union, the United States of America (including its individual states), or any other countries where EBI conducts business or provides services.

Security Incident

- Notice of Security Breach
    - Distributor shall notify EBI's designated contact of any Security Incident including any suspected or known data breach of Distributor Systems as soon as possible but no later than 24 hours after discovery. Notification applies to any Distributor System including those used to process, transmit, or store EBI Restricted Information.

- Distributor Liability

  By receiving the Services, Distributor agrees:
    - To be liable for and reimburse EBI in respect of all claims, liabilities, costs and expenses incurred by EBI and/or its Affiliates related directly to any Security Incident that is caused by the actions or inactions of Distributor and/or Distributor's Affiliates or sub-distributors.
    - To cooperate to EBI's satisfaction in all investigations relating to a Security Incident and to take immediate action to end or prevent any additional loss or damage to EBI Restricted Information.
    - To provide EBI with a copy of any investigative report prepared, either by a third party or internally, no less than 24 hours after such document is available within Distributor.
    - To maintain a current and continuously updated cybersecurity policy used to prevent Security Incidents and ensure the confidentiality, integrity, and availability of any EBI Restricted Information.
    - To include a written response program addressing the appropriate remedial measures it shall undertake if there is a Security Incident.

Enforcement

Any Distributor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Definitions

"Affiliates"
Any entity controlling (directly or indirectly), controlled by or under common control with EBI or Distributor, as the case may be. For the purposes of this definition, "**control**" means direct or indirect beneficial ownership of more than 50% of the share capital, stock or other participating interest carrying the right to vote or to distribution of profits of that entity or person, as the case may be.

"Confidential Information"
All confidential or proprietary information of a person (including of EBI and Distributor, and their respective Affiliates, as the case may be) in oral, written, graphic, electronic or other form including, but not limited to, past, present and future business, financial and commercial information, business concepts, trade secrets, prices and pricing methods, marketing and customer information, financial forecasts and projections, technical data and information, formulae, analyses, trade secrets, ideas, methods, processes, know-how, computer programs, products, equipment, product road maps, prototypes, samples, designs, data sheets, schematics, configurations, specifications, techniques, drawings, and any other similarly sensitive data.

"Distributor"
Any person or entity to whom EBI provides any wholesale satellite broadband services from time to time whether directly or indirectly, and including any Distributor Affiliate and sub-distributor involved in receiving the Services from EBI. For the avoidance of doubt this excludes any end users with whom EBI has a direct retail relationship.

"EBI"
Euro Broadband Infrastructure Sarl, a company within the Viasat group of companies, incorporated in Switzerland whose principal office is at EPFL Innovation Park, Bâtiment J, 1015 Lausanne, Switzerland and with company registration number CHE-144.804.116.

"EBI Information Resource"
Software, hardware, information and materials, and other services and technologies used or utilized by Distributor in receiving the Services and performing its obligations under all and any agreements entered into between EBI and Distributor from time to time.

"EBI Restricted Information"
Any Confidential Information relating to EBI or any of its Affiliates, end user data, other data, or information regardless of form, provided to, used by, or made available to Distributor by EBI or on EBI's behalf. This includes Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), payment card and cardholder information, financial information of EBI or any EBI Affiliate, IPR of EBI or any EBI Affiliate, and other EBI or EBI Affiliate non-public or confidential information.

"IPR"
Patents, petty patents, utility models, registered and unregistered trademarks, trade names and business names, registered designs, design rights, copyright and neighboring rights, database rights, domain names, and rights in inventions, rights in business information, software, trade secrets and all kinds of Confidential Information and other similar proprietary rights which may subsist in any part of the world and whether registered or not (including applications for registration of such rights and rights to apply for such registrations)

“Security Incident”
Accidental, unauthorized, or unlawful access to, disclosure of, destruction of, alteration of or total or partial loss of EBI Restricted Information. This includes any type or size of data breach.

“Services”
All services provided by EBI to a Distributor (or any Distributor Affiliate and/or any sub-Distributor).

“Distributor Systems”
Distributor's software, hardware, information and materials, and other services and technologies reasonably used or utilized by Distributor in receiving the Services and performing its obligations under all and any agreements entered into between EBI and Distributor from time to time.

“Vulnerability Management Program”
The cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities. The program must include continuous monitoring and mitigation of vulnerabilities including continuously testing for normal, typical, and bad behavior, periodic security audits of Distributor Systems via vulnerability scanning, penetration testing, vulnerability assessments, vulnerability remediation and system/ application patching.

Revision History

Version Number	Description of Change	Change Date	Revision PoC	Approval
1.0.0	Initial Draft	02/01/2023	Grant Tiemann	Mark Colaluca, CISO; Foundational Security Principles Team