CYBERSECURITY

Frequently asked questions about how SES addresses security

FAQ

SES

FAQ

A holistic approach towards cybersecurity by SES

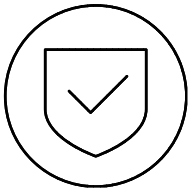
Statistics show that cybersecurity attacks and incidents have increased dramatically over the last few years[1]. Sophisticated cyberattacks such as extensive campaigns using phishing emails, ransomware deployments, or spyware infiltrations are becoming more commonplace. Coupled with the growth in teleworking brought about by the COVID-19 pandemic, these trends have led to public and private-sector organisations from many different sectors (for example – shipping, energy, telecommunications) being targeted and experiencing severe impacts on their everyday business[2].

At SES, we understand the vital role of cybersecurity. That is why our top priority is to provide our customers with the assurance that our services are adequately secured. We follow a holistic approach towards cybersecurity by implementing a wide range of security control mechanisms and practices based on industry-leading standards, as well as cultivating a culture of awareness and caution throughout our organisation.

Below, we explain how SES addresses the cybersecurity questions most frequently asked by our customers.

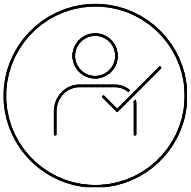
[1] 134 Cybersecurity Statistics and Trends for 2021, Varonis, https://www.varonis.com/blog/cybersecurity-statistics/

[2] Significant Cyber Events List, Center for Strategic and International Studies, csis-website-prod.s3.amazonaws.com



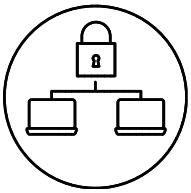
1. How does SES organise and manage information security?

We prioritise information security by establishing, maintaining, and continually improving our Information Security Management System (ISMS). This enables us to implement information security control mechanisms and practices in a consistent, organised and comprehensive manner. In addition, by certifying our ISMS in accordance with ISO/IEC 27001 and continually expanding its scope, we are able to assure our customers that our IT systems and satellite services are well protected.



2. How does SES manage user accounts?

We have defined and implemented formal processes for the arrival, transfer, and departure of our employees to ensure that only authorised personnel can access our IT and operations systems. In addition, through our granular, Role-Based Access Control (RBAC) model, we grant our employees access to only the resources and IT systems that they need in order to perform their assigned tasks.



3. How does SES enforce the use of strong passwords?

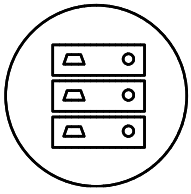
Passwords do not have to be a weak point for organisations; on the contrary, through the implementation of password policies based on best practices and industry standards for different types of accounts (for example – regular users, administrators, etc.), we can offer the assurance that strong passwords are enforced. The use of Multi-Factor Authentication (MFA) for privileged accounts offers an additional layer of defence.

4. How are SES's employees made aware of cybersecurity risks?

We believe that security awareness plays a crucial role in protecting our systems. For this reason, we equip all our employees with the tools and awareness they need in order to identify and react to potential information security incidents and events. To keep our users engaged, we deliver our security awareness training through a variety of methods, including classroom training and e-learning modules. We stay ahead of current trends by reviewing our security awareness content regularly, ensuring it remains up to date when addressing cybersecurity threats and challenges.

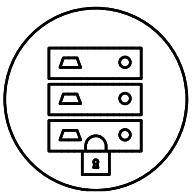
5. How does SES address risks arising from the use of mobile devices in the teleworking era?

As more and more people are teleworking, we pay particular attention to safeguarding our employees' mobile devices by utilising numerous security control mechanisms, ranging from the protection of data on mobile devices to full disk encryption on laptops. We equip our employees with mobile devices that are securely configured so that they will not be the 'weakest link'.



6. How does SES secure data consistently, depending on their level of criticality?

To ensure that data is handled with appropriate care and safeguarded based on its criticality/sensitivity, we have developed a classification scheme, in accordance with which we apply appropriate security controls for each level of information.



7. How does SES protect customer data from being disclosed or intercepted?

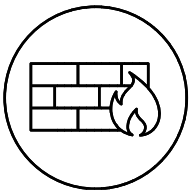
Depending on the sensitivity of data, we implement cryptographic controls using a risk-based approach and follow best practices to protect it from disclosure to unauthorised third parties.

8. Does SES dispose of media securely?

We follow best-practice and/or legally mandated processes to ensure that physical and digital media is disposed of or destroyed securely, preserving the confidentiality of both SES's and our customers' data.

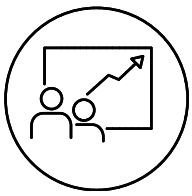
9. How does SES secure its networks and systems?

Our network of information systems and the accompanying communications infrastructure are critical to our ability to provide our customers with the unrivalled next-generation services that they rely on. Our networks are designed with security in mind, with high availability and access only by authorised users. Through a defence-in-depth approach, we implement numerous layers of security controls, including multiple layers of firewalls, application gateways, and state-of-the-art antivirus tools, coupled with Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).



10. How does SES identify and mitigate new risks?

To ensure we are prepared for unanticipated vulnerabilities, we operate an internally managed platform from a market-leading vendor that is complemented by a series of independently conducted external penetration tests. Our systems are continually scanned for vulnerabilities, and our IT security experts perform regular proactive threat watch activities using cyberthreat intelligence feeds.

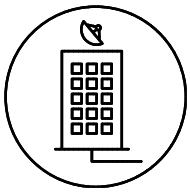


11. How does SES ensure that incidents are identified and managed as soon as possible?

Cybersecurity is an around-the-clock task. That is why we have a centralised, state-of-the-art Security Information and Event Management (SIEM) platform, supported by a team of experienced personnel. The team is responsible for 24/7/365 monitoring and log reviews, as well as performing analyses of SIEM alerts and incident handling and reporting. These activities follow our established information security incident management process, which is aligned with the ISO/IEC 27035 standard.

12. Does SES have a Business Continuity Plan (BCP) that ensures operations are maintained in the event of a major incident?

To assure our clients that their businesses will continue to operate effectively after an incident, we have established a BCP. The plan is supported by backup capabilities and restoration tests that enable us to deliver contractually agreed service quality and availability, as defined in our Service Level Agreements (SLAs). A risk-based assessment of the relevant Information and Communications Technologies (ICTs) has been carried out and recovery targets have been defined in terms of both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).



13. What physical security controls are in place at the sites where SES's data is stored and processed?

Our priority is the security of the physical locations where our customer's data is stored and processed. Our satellite operations and teleport sites are built as 'fortresses' with high-protection security controls (for example – fences and barriers, access controls, CCTV, and guards), in compliance with strict security standards and best practices.

Leverage our robust information security framework to build cyber resilience for your business.

LEARN MORE

SES HEADQUARTERS

Château de Betzdorf
L-6815 Betzdorf
Luxembourg

Published in December 2021.

For more information about SES, visit www.ses.com

SES