Data Security and Encryption Policy

Airbus DS Communications, Inc.

REVISION HISTORY

Date	Version	Author	Change
04-07-2016	1	Ryan Christensen	

© 2016 Airbus DS Communications, Inc. This document is protected by copyright law and international treaties, and is the CONFIDENTIAL AND PROPRIETARY information of Airbus DS Communications, Inc. Unauthorized reproduction, use, or distribution of this document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. All trademarks, service marks, product names, brands, company names and logos appearing in this proposal are the property of their respective owners.

At Airbus DS Communications, Inc. ("Airbus DS Communications"), we are always conscious and respectful of personal privacy. The following is an overview of our data security and encryption policies regarding our hosting of and interaction with customer data through the performance of our services.

Data Security Policy

Purpose

This document defines the policy to secure customer data at Airbus DS Communications, from first receipt for as long as that data is managed by Airbus DS Communications, or until such data is destroyed. These measures primarily guide in controlling access to customer data and backup/recovery procedures for this data. Airbus DS Communications maintains a commitment to protect each customer's data.

Scope

These policies apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, administration, and transportation of hosted customer data. No individual who supports these entities or processes shall be exempt from this policy.

Policy

This Data Security Policy governs the collection, management, and disposal of data, both emergency notification and operational, shared with Airbus DS Communications by its customers.

Data Security shall include the following:

1. All customer data will be backed up to a removable or offsite media on a daily basis.

2. Customer data will be backed up in a manner that permits full recovery to any specified date. These recoveries will include the ability to recover system configuration settings, such as registry settings.

3. If data is backed up to removable media, that media will be rotated offsite at least weekly, preferably daily.

4. All sensitive customer data is stored on secured hosting center production servers.

5. Airbus DS Communications will provide a fax machine in a secured location for transmitting sensitive data.

6. Customer data will only be transferred across secure communications media, unless explicitly requested otherwise by the customer.

© 2016 Airbus DS Communications, Inc. This document is protected by copyright law and international treaties, and is the CONFIDENTIAL AND PROPRIETARY information of Airbus DS Communications, Inc. Unauthorized reproduction, use, or distribution of this document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. All trademarks, service marks, product names, brands, company names and logos appearing in this proposal are the property of their respective owners.

7. A separation of duties shall exist between individuals who authorize data access and personnel who enable data access.

8. When an employee or contractor's services are terminated, their system access is terminated as a result of Airbus DS Communications *Employee/Contractor Termination Policy*.

9. When data or hardware that stores data classified as "Airbus DS Communications Hosting Center Confidential" which is defined in the "Information Sensitivity Policy" reaches its EOL, it must be disposed of in a secure manor that prohibits the retrieval of the data by unauthorized parties. EOL is defined as the permanent decommissioning of hardware from a functioning state or the state of customer data after contract termination.

10. Hardware that is to be re-purposed that contains confidential data must be sanitized in the following manner.

a. All internal storage devices that are to be reused that contain confidential data must be subjected to a process that over writes the entire storage area of the device with a minimum of three passes of random data;
b. If the storage devices of a hardware system are to be decommissioned, they will be physically destroyed.
c. Backup media including magnetic tape, optical media and paper will be physically destroyed when it reaches its EOL

Encryption Policy

Purpose

The Purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have proven to work effectively. Additionally, this policy provides direction to ensure that federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the Unites States of America.

Scope

This policy applies to all Airbus DS Communications employees and customers.

Policy

Proven, standard algorithms such as 3DES, DES, Blowfish, RSA, RC5, and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. Airbus DS

© 2016 Airbus DS Communications, Inc. This document is protected by copyright law and international treaties, and is the CONFIDENTIAL AND PROPRIETARY information of Airbus DS Communications, Inc. Unauthorized reproduction, use, or distribution of this document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. All trademarks, service marks, product names, brands, company names and logos appearing in this proposal are the property of their respective owners.

Communications key length requirements will be reviewed annually and upgraded as technology allows. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Airbus DS Communications. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Standards and Key Management

1. The standard that Airbus DS Communications uses involving encryption and Key Management is as follows:

   2048 bits SSL encryption on all web interfaces; SSL signatures shall be used with sha1RSA, 2048 bit encryption, Public Key. HTTPS shall be 2048 bit security. Data transferred to and from servers is transferred using Digital Signature, Key Encipherment, and Data Encipherment.

2. Data will be encrypted before being stored offsite.

3. Copies of public keys are kept offline located in a fireproof safe on encrypted q media. Each VPN Tunnel uses 168 bit 3DES encryption and HMAC MD5 authentication is used to verify integrity.

Airbus DS Communications complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries to the extent applicable to our contracted services. We adhere to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view the our certification, please visit http://www.export.gov/safeharbor/

© 2016 Airbus DS Communications, Inc. This document is protected by copyright law and international treaties, and is the CONFIDENTIAL AND PROPRIETARY information of Airbus DS Communications, Inc. Unauthorized reproduction, use, or distribution of this document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. All trademarks, service marks, product names, brands, company names and logos appearing in this proposal are the property of their respective owners.