



ACCESSYSTEM

Global Security & Privacy Practices

Providing Solution for Small Business & Mid-Level Enterprise.
YOUR BUSINESS IS OUR JOB
www.accessystem.com

ACCESSYSTEM



Complete IT Solution & Services

Global Security & Privacy Practices

ACCESSYSTEM® shall maintain and implement the following technical and organizational measures in relation to the security of Customer Configuration. In all cases, the Customer remains the primary system/account administrator and is responsible for protecting Customer Data by (i) selecting and purchasing appropriate security appliances as part of the Services (ii) implementing appropriate encryption and logical access controls and (iii) maintaining appropriate application security controls. Certain ACCESSYSTEM® services are available to help Customer's meet these requirements.

1. Physical Security - Data Centers. The following physical security controls apply to ACCESSYSTEM®'s provision of dedicated Hosting Services (Managed, Managed Colocation, and Intensive® service levels/segments) and the ACCESSYSTEM® Public Cloud Services.

1.1 Servers and devices dedicated to your use as part of a Hosted System provided by ACCESSYSTEM® will be located in a controlled access data center (or portion thereof) either operated by or dedicated to use by ACCESSYSTEM® US, Inc. or a ACCESSYSTEM® affiliated company.

1.2 ACCESSYSTEM® operates or audits the use of an Electronic Access Control System managed by a professional security guard force in line with its current processes. Access logs are retained for a period of at least twelve (12) months.

1.3 Access to the raised production floor of the data halls will be restricted to ACCESSYSTEM® employees or its agents who need access for the purpose of providing the Services. Access within data center facilities is in zones and provisioned based on physical access rights required by a given individual. Access to designated "meet me" rooms will be available to customers, subject to data center escort policies.

1.4 The data center will be staffed 24/7/365 and will be monitored by video surveillance, recording to a centralized location and viewed by the onsite security force.

1.5 Entrance to the data center will be authorized by proximity-based access cards and biometric hand scanners or other approved security authentication methods.

1.6 The data centers from which ACCESSYSTEM® provides dedicated Hosting Services are identified on your applicable Service Description or Service Order by their nearest airport code. Except as specifically provided for in any applicable Product Terms ACCESSYSTEM® will not relocate your Hosted System to a data center in another country without your express written permission.

1.7 Following the termination of your Agreement for a Hosted System, ACCESSYSTEM® will wipe data from those hard drives and storage devices dedicated to your use prior to re-use.

2. Security Controls Audits & Reporting. ACCESSYSTEM® shall engage qualified third party auditors to perform examinations of its systems and services in accordance with: the best practice recommendations of ISO 27002, for the purpose of auditing ACCESSYSTEM®'s compliance with ISO 27001; SSAE 16 and ISAE 3402 compliance frameworks, and the AT 101 compliance framework (based upon select Trust Services Principles); and/or equivalent industry standards. ACCESSYSTEM®'s annual SOC report(s) or suitable equivalent standard(s) as specified by ACCESSYSTEM® is available to Customer upon the Customer's request subject to ACCESSYSTEM®'s SOC distribution requirements. Not all ACCESSYSTEM® Services are included in the scope of the SOC report(s) or audits described above, for details please contact your account manager.

3. Administrative Controls

3.1 Screening. ACCESSYSTEM® will perform pre-employment background screening of its employees who have access to customers' accounts, and is committed to employee supervision, training, and management.

3.2 ACCESSYSTEM® Access. ACCESSYSTEM® will restrict the use of administrative access codes for customer accounts to its employees and other agents who need the access codes for the purpose of providing the Services. ACCESSYSTEM® personnel who use access codes shall be required to log on using an assigned user name and password.

3.3 Customer Access. As the primary system administrator, the customer is responsible for the management of their accounts, including creation, change management, and termination, and enforcement of related remote working and password controls.

4. PCI-DSS. With respect to the security of cardholder data, as that term is defined in the Payment Card Industry-Data Security Standard, we may possess or otherwise store, process or transmit on Customer's behalf, ACCESSYSTEM® agrees to provide (i) those physical, technical, and administrative safeguards described in your Agreement with ACCESSYSTEM® and

(ii) the Services selected by you and described in the applicable Service Description; provided that Customer remains responsible for ensuring all PCI-DSS requirements are met with respect to such cardholder data. ACCESSYSTEM® maintains PCI-DSS Service Provider, or equivalent, accreditation with regards to dedicated infrastructure Hosting Services (excluding managed virtualization services).

5. Reports of and Response to Security Breach. ACCESSYSTEM® will report to you as soon as reasonably practicable in writing and in accordance with applicable law, of a material breach of the security of your Customer Configuration or Hosted System which results in unauthorized access to your Customer Data resulting in the destruction, loss, unauthorized disclosure or alteration of your data of which we become aware. Upon request, we will promptly provide to you all relevant information and documentation that we have available to us regarding your Customer Configuration or Hosted System in connection with any such event.

6. Customer Data Return. The Services enable you to retrieve, correct, or delete Customer Data. Depending on your Services, you may not have access to your Customer Configuration or Customer Data during a suspension of Services, or following the termination of the Agreement. You are responsible for retrieving a copy of your Customer Data prior to the termination of the Agreement.

7. Privacy and Personal Data Processing.

7.1 Roles. In respect to Personal Data processed under the Services, Customer may act as "controller" or "processor" and ACCESSYSTEM® may act as "processor" or "subprocessor," as those terms are defined in the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Customer is responsible for integrity, security, maintenance and appropriate protection of Personal Data. ACCESSYSTEM® is responsible for those security measures detailed here or in the applicable Agreement.

7.2 Instructions for Data Processing. ACCESSYSTEM® will process Personal Data only to the extent and in such a manner as is necessary to provide the Services under the Agreement or as otherwise instructed by Customer from time to time.

7.3 Notifications. ACCESSYSTEM® shall notify the Customer as soon as reasonably practicable in writing: (a) of any communication received from an individual relating to (i) an individual's rights to access, modify, correct, delete or block his or her Personal Data and (ii) any complaint about Customer's Processing of Personal Data; and (b) to the extent not prohibited by law, of any complaint, notice or other communication that relates to Customer's compliance with data protection and privacy law and the processing of Personal Data.

Customer agrees to make any required notifications to and obtain required consents and rights from, individuals in relation to ACCESSYSTEM®'s provision of any work or Services to Customer. Where ACCESSYSTEM® receives the communication described in this section and notifies Customer of such communication, it is Customer's responsibility to respond to and take all other appropriate action with regard to the communication required under the applicable law.

7.4 Personal Data Transfer from the European Economic Area and Switzerland to a ACCESSYSTEM® entity located in India.

7.4.1 ACCESSYSTEM®'s participation in the Privacy Shield Program. ACCESSYSTEM® US, Inc. and its controlled US subsidiary (Objectrocket, LLC, collectively "ACCESSYSTEM®") participate and have certified its compliance with the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Frameworks ("Privacy Shield"), as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data transferred from the European Union, European Economic Area, and Switzerland to the United States.

ACCESSYSTEM®'s participation in the Privacy Shield program is applicable to all Personal Information that is subject to the ACCESSYSTEM® Privacy Statement. The scope of ACCESSYSTEM® compliance with the Frameworks' Privacy Principles is described in the ACCESSYSTEM® Privacy Shield Notice.

To learn more about and to view these ACCESSYSTEM® certifications, please visit <https://www.privacyshield.gov/list>.

7.4.2 Personal Data Customers Process When Using ACCESSYSTEM® Services. ACCESSYSTEM® provides the Services under the direction of its customers and has no direct relationship with the individuals whose Personal Data its customers process when using the Services. ACCESSYSTEM® does not determine the Customer Data collected, stored, and transmitted by its customers using the Services. In these situations, it is its customers rather than ACCESSYSTEM® who decide how Customer Data is classified, accessed, exchanged or the reasons for which the Customer Data will be processed. Consistent with the EU-U.S. Privacy Shield and Swiss

-U.S. Privacy Shield Framework, the extent to which ACCESSYSTEM® can apply the Privacy Principles is limited when ACCESSYSTEM® customers use the Services to process their Customer Data. Therefore, you are responsible for complying with the Privacy Principles regarding Personal Data that have originated in the European Union, European Economic Area, and Switzerland.

ACCESSYSTEM® defines its obligations with respect to Customer Data in the Agreement and this Global Security and Privacy Practices. As stipulated in the supplementary Privacy Shield Principle 10 ("Obligatory Contracts for Onward Transfers"), because adequate protection is provided by Privacy Shield participants, contracts with Privacy Shield participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the EU Member States), as would be required for contracts with recipients not participating in the Privacy Shield or otherwise not providing adequate protection.

If ACCESSYSTEM® subcontractors have access to Customer Data in the course of provision of their services, such subcontractors enter into a written agreement with ACCESSYSTEM® that requires them to maintain security and confidentiality practices that are consistent with the Agreement and ACCESSYSTEM®'s privacy and information security practices and policies, as applicable.

When ACCESSYSTEM® uses subcontractors for the provision of its Services, ACCESSYSTEM® complies with the Accountability for Onward Transfer Privacy Shield Principle, as applicable.

Source URL: <http://www.accesssystem.com/legal/securitypractices.html>