ACCOR

General IT Security Policy

Version Status

This version of this document is currently:

	In Progress
	In Review
⇒	**Published**

Document History

Version	Authors	Reviewers	Publisher	Date	Changes
0.7	MSW	ATR		18 March 2013	Initial version
1.0		SAG	ATR	13 May 2013	Validated
1.1	ATR		ATR	17 July 2014	Clarified requirement to review hardening guides annually
1.2			ATR	27 October 2014	Annual review. PCI V3.0 update
1.2.1	ATR		ATR	21 November 2014	Specified what “strong encryption” means for sending card data over public networks
1.2.2		Pierre AURE		4 March 2016	Annual review : minor updates / typography
1.2.3		Pierre AURE		17 March 2017	Annual review
1.2.4		Pierre AURE		14 March 2018	Annual review
1.3		Pierre AURE		29 March 2019	Annual review
1.4		Pierre AURE		26 Feb 2020	Annual review
1.5		Pierre AURE		11 June 2020	Masking precision

Projected Review Date

1 year after the most recent publication

This Document

Context	This document describes Accor's information technology security policy.
Contents	This document contains the set of policies for domains, areas, and aspects of Accor's IT security.
Audience	This document is written for the complete set of stakeholders in the Accor community, including employees, contractors, interns, and suppliers.
Sources	These policies are based on field experience and industry best practices, as well as on the set of information security policy templates from the SANS Institute: http://www.sans.org/security-resources/policies/
Related Documentation	The set of Security Policies and Procedures documents are currently available from the Accor intranet at the links: http://acsa.accor.net/dgsit/pci/Documents/Livrables https://pci.accor.net
Using this guide	This document presents guidance and principles rather than specific procedures. It is designed to be read and implemented in a context that is co-defined in the complete set of security documentation.
What's not in this document	This document is not by itself an exhaustive guide to or definition of Accor security policy. Refer to the list specified in *Related Documentation* above.
Questions?	Contact security@accor.com
Copyright	© Accor All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission from Accor. For permission requests, write to security@accor.com

Abbreviations used in this document

ASV	Approved Scanning Vendor
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
DSS	Data Security Standards
ISM	Infrastructure Security Manager
IT	Information Technology
PCI	Payment Card Industry
QSA	Qualified Security Assessor
TBD	To be defined

Table of Contents

1 Accor Security Policy

1.1 Context

In a general context of worldwide economic competition, the Accor Group must protect its know-how and its informational capital. Accor is also committed to protecting the personal information of its guests, collected and processed in Accor systems.

The human, technical, industrial and financial consequences of dysfunctions or malicious activities must be known, monitored, and managed, while still ensuring the desired level of transparency.

1.1.1 Analyses

The Information Security Policy must be defined around multiple analyses, including in particular:

- Current and future information systems;
- Vulnerabilities that could impact missions and operations that are critical for Accor Group;
- Expected threats;
- Existing security measures.

1.1.2 Threats and Risks

Information security can only be applied in an environment where risks have been identified, even if only in the broadest terms. It is impossible in a document of this length to do more than summarize and highlight the risks and threats to Accor Group.

- **Accidents**, such as:
  - Physical issues (fire, earthquake, etc.)
  - Power or telecom networks unavailability.
- **Errors**, such as:
  - Infrastructure design or administration errors
  - Software design or implementation errors (bugs).
- **Malicious activities**, such as:
  - Abuse of privilege, confidential information disclosure
  - Physical attack (on systems, buildings, etc.)
  - Logical attack (on infrastructure, software, etc.).

1.2 Policy Objective

The goal of this document is to define the principles and guidelines for adoption in Accor to make sure that information is protected in a way that is:

- Flexible - Effective policy needs to be able to meet the current needs of the organization as well as future needs by accommodating changes in technology and the organization’s threat model.
- Relevant - The policy must reflect the business goals of the organization.
- Applicable - The policy must reflect the realities of the environment.

- Feasible - Goals should be measurable and attainable.
- Timely - The policy should be current, reflecting recent developments in factors both external and internal to the organization.
- Cost-effective - The policy should be cost-effective. Effort and materials expended should be in proportion to the value of the assets they are meant to safeguard.
- Enforceable - The policy should be enforceable. While the policy is not intended to dictate the method of implementation, defining policy that is not possible to implement creates confusion and wasted effort.
- Possible - The policy should integrate well with the existing organizational policy.

1.3 Scope

The Information Technology (IT) Security Policies apply to all information obtained, created, or maintained by Accor's information resources and systems. These Policies apply equally to all levels of management and to the personnel they supervise. Further, these Policies apply to all information generated by Accor's Information Resources functions, from the time of creation through the time of transfer to ownership external to Accor or its proper disposal/destruction.

1.4 Applicability

These Policies apply equally to all personnel, including, but not limited to, Accor's employees, agents, consultants, contractors, volunteers, vendors, business partners, and all other authorized users granted access to Information Resources.

In this policy, these persons are described as "*Accor-internal stakeholders*".

The Accor IT Security Policy must be applied immediately after its official publication by all entities, brands and activities that belong to the Group. External companies, services and products providers must also be in accordance with this Policy when providing products, services or human resources to an Accor-owned company.

Adherence to these policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.

1.5 Availability

The most current version of this policy is available to all Accor-internal stakeholders from the corporate Intranet (IT / Security section).

1.6 Exceptions

The Accor IT Security Team must approve in advance any exceptions to any approved policy.

1.6.1 Nature of exceptions

Exceptions are of two types:

1. An exception may be granted to address the specific circumstances or business needs relating to an individual program or department. Requests for exceptions of this type should be in writing (email is acceptable) and should be initiated by the data owner.
2. Broader exceptions may be issued to cover circumstances that span the entity as a whole. Requests for exceptions of this type may come from any person, or such exceptions may be initiated by the CISO.

1.6.2 Granting exceptions

The data owner and the Digital Services Security Team must approve and document all exceptions, based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure and the potential adverse consequences for individuals, other organizations, or the Accor group if exposure occurs as a result of the exception.

As a condition for granting an exception, the Chief Information Security Officer (CISO) for a specific department may require the implementation of compensating controls to offset the risk created by the exception.

1.7 Security Principles

Accor must manage informational risks in the same terms as any other risks, whether legal, financial, operational, social, penal and so on. This section outlines the essential principles that underlie the set of Accor security policies and procedures. The security policy must:

- Identify information security objectives and risks for all major systems and applications. Security measures must be compliant with the identified risks.
- Establish a thorough control system for information security, protecting information resources from unauthorized access, leakage, falsification, loss, destruction, or interruption of operation.
- Establish administrative control for information security in a management framework that ensures the confidentiality, integrity and availability of information. As part of that framework, Accor-internal stakeholders must be brought to understand that they are responsible for their decisions and actions.
- Advance the understanding of and generalize the responsibility for information security, through information security education and training.
- Make the best use of existing solutions (organization, procedures, hardware and software) whenever possible.
- Avoid impacts on the availability of the operational infrastructures.
- Include security in the lifecycle of projects and services.
- Consider security as a process, not a one-time action, in particular through regular reviews in response to rapid changes in the environment.
- Define the information access rights in accordance with the “Least privilege principle” and “need to know” basis.

- Implement and maintain internal controls through monitoring and internal audits.
- Enforce control over third parties, negotiating contracts with outside parties that satisfy reliability requirements for such operations, and periodically monitoring and reporting on the activities and work of outside parties to prevent the leakage of information.

1.8 Responsibility

1.8.1 Responsibility for Security Policies

Overall responsibility for creating, communicating, distributing, maintaining, and enforcing Security Policies lies jointly with:

- Human Resources Department
- Chief Information Security Officer (CISO)

1.8.2 Responsibility for Information Security

Within Accor, responsibility for matters relating to information security lies with the **Chief Information Security Officer**.

This role has responsibility for:

- Overall responsibility for Information Security and related issues;
- Development and maintenance of Information Security Policies and Procedures (including distribution to and training of, staff in policies);
- Overall monitoring and analysis of security alerts, and distribution to appropriate Accor personnel;
- Keeping IT security staff and management updated on all security-related issues.
- Coordination of compliance-related activities (such as PCI DSS).

1.8.3 Responsibilities of Associated Teams

General Management

The General Management of the Accor Group is primarily responsible for its informational assets, and must, therefore:

- Administrate the Information Security in accordance with the Security Policy and according to local laws and regulations;
- Assume the costs linked to Security and its management.

Countries / Brand managers

The countries/brand managers have to guarantee the application and the control of Information Security within their domain of responsibility.

Operations and IT managers

The operations and IT managers must participate in the application and the control of Information Security as permanent actors. They must define procedures for administrating user accounts, including additions, deletions and modifications.

IT teams

All IT teams must maintain daily administrative and technical operational security procedures that are consistent with the Accor IT Security Policy.

Internal IT Audit team

The Internal IT Audit team must regularly check compliance with the Accor IT Security Policy.

Risk Management Team

The Risk Management Team must include IT security risks in a formal risk assessment process.

General Employees

All Accor-internal stakeholders are responsible for managing their use of IT and are accountable for their actions relating to IT security. Personnel is also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

Passwords, Personal Identification Numbers (PIN), Security Tokens (such as smartcards or VPN tokens), and other computer systems security procedures and devices must be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations must be reported to the custodian or owner department management.

The security awareness of personnel must be continually emphasized, reinforced, updated and validated.

Third Parties

Partners, and Services and Product Providers must conform to the Accor IT Security Policy.

1.9 Incident Management

1.9.1 Nature of Incidents

Security incidents include, but are not limited to virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, data breaches, as well as complaints of improper use of Information Resources as outlined in other Policy documents such as the *IT Usage Policy*.

1.9.2 Responsibilities

In the event of an incident, the person in charge of the impacted system or data is responsible for reporting it to the corporate IT security team.

1.9.3 Procedures

The procedures to execute for detecting, reporting, and responding to security incidents are the subject of a separate Accor document, *Security Incident Response Plan*.[1]

1.10 Protecting Cardholder Data

Cardholder data are governed by the Payment Card Industry Data Security Standard (PCI DSS). As a result, all card processing activities must be conducted in accordance with this standard, as described herein.

No activity may be conducted, nor any technology employed that might obstruct compliance with any portion of the PCI DSS.

PCI DSS applies to all business processes related to cardholder data and to all IT systems involved in **processing**, **storing** or **transmitting** cardholder data. Such systems are considered to be "**in the PCI DSS scope**".

All the following requirements must be respected in the PCI DSS scope. Processes and system documentation must specify how each requirement is implemented.

Goal	#	**Requirement**
Build and Maintain a Secure Network and Systems	1 2	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied for system passwords and other security parameters
Protect Cardholder Data	3 4	Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5 6	Protect all systems against malware and regularly update anti-virus software or programs Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7 8 9	Restrict access to cardholder data by business need to know Identify and authenticate access to system components Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10 11	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel

[1] *Document in progress at the time of writing.*

1.10.1 Network security and firewalls

All systems in the PCI DSS scope must strictly respect the Accor *Network Security Policy*, in particular:

- Documentation (with business justification) and approval process for opening all network connections and flows. Firewall rules must be reviewed at least every six months;
- Network segmentation between untrusted networks, DMZ and internal networks by stateful firewalls;
- Limitation of inbound and outbound traffic to that which is strictly necessary, prohibiting direct connections between public networks and the cardholder data environment.

To facilitate compliance, systems in the PCI DSS scope should be isolated from out-of-scope systems. Isolations mechanisms must be tested at least annually during an internal penetration test.

1.10.2 Configuration standards and patch management

Configuration standards must be maintained for applications, network components, critical servers, and wireless access points in the PCI DSS scope. These standards must be consistent with industry-accepted hardening standards and reviewed annually, even when there isn't any modification to do (in this case, the document header must be updated to justify that review has been done).

System components and applications must be protected from known vulnerabilities by having the latest vendor-supplied security patches installed.

1.10.3 Handling of Cardholder Data

A formal data retention policy must be written to identify what data needs to be retained, for how long and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. **Cardholder data storage must never exceed the business need.**

This retention policy must cover all storage of cardholder data, including electronic storage (databases, servers, files, etc.), hard copies and backup media.

Storage of sensitive card authentication data (magnetic stripe data, card validation code or value, and PIN) after authorization **is prohibited**. Any manipulation of such data within Accor must be validated by the Accor PCI DSS Management Committee.

The handling of payment card Primary Account Numbers (PANs) requires attention:

- PANs must be rendered unreadable anywhere they are stored.
- Access to unencrypted card data must be strictly restricted to selected personal based on the "need to know" justification. When displaying cardholder data, the PAN must be masked according to the applicable standards[2] and obligations.
- Unencrypted PANs may not be sent via email. Strong cryptography (ie. only with trusted certificates, with secure versions of the encryption protocols and associated with a

[2] PCI DSS : https://www.pcisecuritystandards.org/document_library

certificate renewal process) must be used during the transmission of cardholder data over open networks.

1.10.4 Access to Cardholder Data

Procedures for data control must be maintained by each department and must incorporate the following:

- Access rights to privileged User IDs are restricted to the least privileges necessary to perform job responsibilities;
- Assignment of privileges is based on job classification for individual personnel, and should only be granted after management approval;
- Use of generic and shared accounts is forbidden;
- A strict password policy (as detailed in PCI DSS Requirement 8) must be enforced.

Moreover, before hiring personnel with cardholder data access, screening should be performed, consistent with local legal requirements.

1.10.5 Antiviruses

All systems commonly affected by malicious software (in particular, at the time of writing, Microsoft Windows and Linux systems) must be actively protected by antivirus software. This antivirus software must generate audit logs. Signatures must be up to date.

1.10.6 Change & patch management

In the PCI DSS scope, a strict change management process must be in place, including change documentation and a formal approval process.

Moreover, a formal process must be in place to ensure that system and software components are protected from known vulnerabilities by having security patches installed.

1.10.7 Application security

To help prevent the creation of coding vulnerabilities, the Accor IT Security Policy must be strictly enforced on all custom applications in the PCI DSS scope.

1.10.8 Physical security

Physical security measures must be in place to permit access control and traceability on physical media and servers that contain cardholder data.

1.10.9 Logging

All-access to cardholder data and all administration actions in the PCI DSS scope must be tracked. Log files must be protected against unauthorized modification and kept for at least one year. Logs must be reviewed daily.

1.10.10 Security controls

Security controls must be in place in the PCI DSS scope, including:

- Rogue access points detection;
- Vulnerability scans;
- Penetration tests;
- Intrusion Detection System;
- File Integrity Monitoring.

1.10.11 Partners and third parties

Partners and third parties involved in cardholder data manipulation on behalf of Accor are a source of risk. Before contracting with such providers, the following process must be followed:

- Due diligence must be carried out, to validate the provider's security level, at least through a penetration test.
- A written agreement must include the acknowledgement that the service provider is responsible for the security of cardholder data.

A list of service providers must be maintained, and an annual process applied to monitor their PCI DSS compliance status.

1.10.12 Security controls review

At least quarterly, security controls implemented must be a review to verify that the security policy and operational procedures are followed in accordance with each dedicated process:

- Daily log reviews;
- Firewall rule-set reviews;
- Applying configuration standards to new systems;
- Responding to security alerts;
- Change management processes.

1.11 Penalties

Violation of any of the requirements in this policy by any Accor-internal stakeholder will result in suitable disciplinary action, up to and including prosecution and/or termination.

Violation of any of the requirements in this policy by any Visitor can result in similar disciplinary action against the sponsoring employee and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

1.12 Policy Reviews

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.