

NIST SPECIAL PUBLICATION 1800-27A

---

# Securing Property Management Systems

---

**Volume A:**  
**Executive Summary**

**William Newhouse**

Information Technology Laboratory  
National Institute of Standards and Technology

**Michael Ekstrom**

**Jeff Finke**

**Marisa Harriston**

The MITRE Corporation  
McLean, Virginia

September 2020

DRAFT

This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems>



# Executive Summary

1 In recent years criminals and other attackers have compromised the networks of several major hotel  
 2 chains, exposing the information of hundreds of millions of guests. Breaches like these can result in huge  
 3 financial loss, operational disruption, and reputational harm, along with lengthy regulatory  
 4 investigations and litigation. Hospitality organizations can reduce the likelihood of a hotel data breach  
 5 by strengthening the cybersecurity of their property management system (PMS). The PMS is an  
 6 attractive target for attackers because it serves as the information technology (IT) operations and data  
 7 management hub of a hotel. This cybersecurity practice guide shows an approach to securing a PMS and  
 8 the ecosystem of guest services it supports. It offers how-to guidance for building an example solution  
 9 using commercially available products, standards, and best practices for role-based access control,  
 10 privileged access management, network segmentation, moving target defense, and data protection.

## 11 CHALLENGE

12 Hospitality organizations rely on a PMS for  
 13 daily tasks, planning, and record keeping. As  
 14 the operations hub, the PMS interfaces with  
 15 several services and components within a  
 16 hotel’s IT systems, such as point-of-sale (POS)  
 17 systems, physical access control systems,  
 18 Wi-Fi networks, and other guest service

---

*An unsecured or poorly secured PMS could expose a hotel—and the larger hospitality organization of which the hotel is a part— to a significant and costly data breach...*

---

19 applications. A PMS, and the extended PMS ecosystem, stores, processes, and transmits a variety of  
 20 sensitive guest information, including payment card information (PCI) and personally identifiable  
 21 information (PII). An unsecured or poorly secured PMS could expose a hotel – and the larger hospitality  
 22 organization of which the hotel is a part – to a significant and costly data breach, including financial  
 23 penalties for violating state, federal, and international privacy and other regulatory regimes.

24







### *This practice guide can help your organization:*

- **instill consumer confidence and brand loyalty** by protecting guest privacy and payment card information
- **limit the cost** for recovery and mitigation if a breach occurs
- **build the business case**, functional requirements, and test plan for a similar solution within your own environment
- **support privacy/regulatory compliance** by using data tokenization and limiting the spread of data beyond “need-to-know”
- **increase overall PMS security** situational awareness, and limit exposure of the PMS to incidents in systems that interface with it
- **control and limit access** to your PMS to those with a business need

## 25 SOLUTION

26 The National Cybersecurity Center of Excellence (NCCoE) collaborated with the hospitality business  
 27 community and cybersecurity technology providers to build an environment that simulates a hotel's IT  
 28 infrastructure, including guest WiFi and a PMS integrated with a POS module and an electronic door lock  
 29 system. Using commercially-available products, the example solution shows how to protect data moving  
 30 within this environment, and limit or prevent user access to the various systems and services.

31 The example solution uses technologies and security capabilities (shown below) from our project  
 32 collaborators. All technologies used in the solution support security standards and guidelines of the NIST  
 33 Cybersecurity Framework, Hotel Technology Next Generation, and the PCI Security Standards Council,  
 34 among others. Although following the guide does not ensure General Data Protection Regulation (GDPR)  
 35 compliance, the recommended solution aligns with the key principles of GDPR.

Collaborator	Security Capability or Component
	Network protection appliance that provides an additional layer of protection against cyber attacks
	Visualizes the diverse types of devices connected to the network; enforces policy-based controls
	Physical access control ecosystem including door locks, room key encoding, and management
	Real-time incident monitoring and detection, privilege escalation management and reporting functions
	Payment solution appliance that secures credit card transactions and shrinks the PCI compliance enclave
	Access control platform that secures connections, and provides control mechanisms to enterprise systems for authorized users and devices; monitors activity down to the keystroke

36

37 While the NCCoE used a suite of commercial products to address this challenge, this guide does not  
 38 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your  
 39 organization's information security experts should identify the products that will best integrate with  
 40 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that  
 41 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
 42 implementing parts of a solution.

## 43 HOW TO USE THIS GUIDE

44 Depending on your role in your organization, you might use this guide in different ways:

45 **Business decision makers, including chief information security and technology officers** can use this  
46 part of the guide, *NIST SP 1800-27a: Executive Summary*, to understand the impetus for the guide, the  
47 cybersecurity challenge we address, our approach to solving this challenge, and how the solution could  
48 benefit your organization.

49 **Technology, security, and privacy program managers** who are concerned with how to identify,  
50 understand, assess, and mitigate risk can use *NIST SP 1800-27b: Approach, Architecture, and Security*  
51 *Characteristics*, which describes what we built and why, including the risk analysis performed, and the  
52 security/privacy control mappings.

53 **IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-27c: How-*  
54 *To Guides*, which provides specific product installation, configuration, and integration instructions for  
55 building the example implementation, allowing you to replicate all or parts of this project.

## 56 SHARE YOUR FEEDBACK

57 You can view or download the guide at [https://www.nccoe.nist.gov/projects/use-cases/securing-](https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems)  
58 [property-management-systems](https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems). Help the NCCoE make this guide better by sharing your thoughts with  
59 us. If you adopt this solution for your own organization, please share your experience and advice with  
60 us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we  
61 encourage organizations to share lessons learned and best practices for transforming the processes  
62 associated with implementing this guide.

63 To provide comments or to learn more by arranging a demonstration of this example implementation,  
64 contact the NCCoE at [hospitality-nccoe@nist.gov](mailto:hospitality-nccoe@nist.gov).

65

---

## 66 COLLABORATORS

67 Collaborators participating in this project submitted their capabilities in response to an open call in the  
68 Federal Register for all sources of relevant security capabilities from academia and industry (vendors  
69 and integrators). Those respondents with relevant capabilities or product components signed a  
70 Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to  
71 build this example solution.

72 Certain commercial entities, equipment, products, or materials may be identified by name or company  
73 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an  
74 experimental procedure or concept adequately. Such identification is not intended to imply special  
75 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it  
76 intended to imply that the entities, equipment, products, or materials are necessarily the best available  
77 for the purpose.