

*Accor Bangkok Tech Center*



# Accor Bangkok Tech Center Opening Position

01 March 2024

Department	Opening position
Global Support Services	Service Relationship Manager
Global Support Services	Senior IT Specialist – Tech Support
Global Support Services	Senior IT Specialist – Tech Support (Mandarin Speaking)
Global Support Services	IT Specialist – Tech Support (German Speaking)

Department	Opening position
Security	Director, IT Security Infrastructure
Security	Cloud Security Engineer
Security	Cloud Security Engineer, AWS
Security	Cloud Security Engineer, Azure
Security	Security Analyst SOC
Security	Security Analyst Junior SOC
Security	Security Engineer (IT tools)
Security	Security Engineer, SOC
Security	Security Engineer, Expert Firewall
Security	Security Engineer, Firewall Manager
Security	Security Engineer, Infrastructure
Security	Security Engineer, Proxy
Security	Security Engineer, Remote Access specialization
Security	Vulnerability Management Officer

Department	Opening position
Infrastructure & Operations	DevOps Engineer
Infrastructure & Operations	Performance Engineer
Infrastructure & Operations	Cloud Engineer

Department	Opening position
Tech for Hotels	Business Analyst (PGIT)
Tech for Hotels	Guest Technology Sustainability Manager
Tech for Hotels	IT Administration & Governance officer
Tech for Hotels	Property Tech Manager (POS)
Tech for Hotels	Property Tech Manager
Tech for Hotels	Property Tech Specialist
Tech for Hotels	RM Success Lead

Department	Opening position
Tech for Accor teams	Identity engineer / expert
Tech for Accor teams	Expert Data (Azure DataFactory / MS SQL Server Analysis )
Tech for Accor teams	.Net Expert (C#/ Web/ MVC/ Azure/AzureDevOps/ MS SQL Server)

Department	Opening position
Strategy & Performance	Global Projects Communication Manager



1

# *Global Support Services*



## Job title

# Service Relationship Manager

Global Support Services



## Purpose

The Service Relationship Manager is responsible for managing relationships with internal and external stakeholders, ensuring the delivery of high-quality IT services that meet their needs and expectations. This role requires working with cross-functional teams, building, and maintaining strong partnerships, and driving process improvements to enhance the overall customer experience.

## Hierarchical link

Head of Service Relationship Management

Director Service Management MEAPAC

Service Relationship Manager

## Key interactions

Internally: Hubs Head of Technology, Service & Solution Architects, Internal Stakeholders, Service Owners, ITSM Practice Owners (i.e., Change Enablement), Technology / Application Asset Owners, Engineers

Externally: Externally: External Service Providers

## Main responsibilities

- Maintain strong relationships with internal and external stakeholders, including business units, vendors, and partners
- Collaborate with business units to understand their IT service needs and align IT services to meet their requirements
- Ensure service level agreements (SLAs) are met or exceeded, and customer satisfaction is maintained at a high level
- Lead cross-functional teams to drive process improvements and implement best practices to enhance the overall customer experience
- Manage IT service delivery, ensuring that services are delivered in accordance with agreed-upon SLAs and customer expectations are met or exceeded
- Monitor IT service delivery performance metrics and work with IT teams to identify areas for improvement
- Monitor IT service catalogues, ensuring that they are up-to-date and aligned with business requirements
- Manage vendor relationships, ensuring that vendors are meeting contractual obligations and delivering high-quality services
- Prepare IT service delivery reports to senior management, including service level performance, customer satisfaction, and key performance indicators (KPIs)
- Work with IT teams to ensure that IT service delivery processes are documented and communicated to stakeholders
- Keep up to date with industry trends and best practices
- Any other tasks assigned by the Director Service Management MEAPAC.

**Outcomes:** This role is responsible for being the interface between Accor Tech, Global Service Support and external Service Providers of assets and services

## Main difficulties / Key Success factors related to the position

### Major Challenges:

- The position may require occasional work outside of normal business hours to support the geographical support.

### Communication:

- This position will require strong relationship management skills and communication.

## Sizing : Turnover, budget, size of the teams, ...

- Headcount: a number of team members
- No. of customer accounts: MEAPAC Hotels – 1151+

## Profile

### Educational background

- Bachelor's Degree in computer science or related field or equivalent work experience
- Strong knowledge of ITSM frameworks, such as ITIL or equivalent

### Competencies

- Organized and strong attention to detail.
- Excellent communication skill.
- Strong command of written and spoken English.
- Service-oriented, self-motivated and energetic.
- Multicultural awareness and being able to collaborate with people from diverse cultures.
- Flexible and able to embrace and respond to change effectively.
- Can-do attitude. Able to come up with out-of-the-box solutions.
- Good Team working skills and ability to work effectively and contribute to a team.
- Curious and aware of changes in the industry.
- Ability to manage multiple priorities in a challenging environment.
- Strong analytical and critical thinking skills.
- Experience with IT Service Delivery tools and systems.
- Excellent leadership and interpersonal skills.



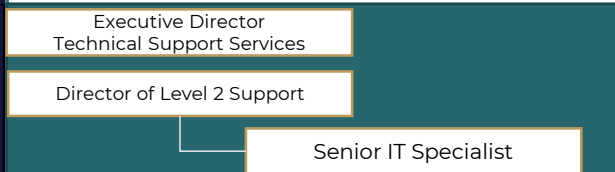
## Job title

Senior IT Specialist – Tech Support Level 2

## Purpose

Senior Specialist plays a critical role in providing expert-level technical support, mentoring junior team members, managing projects, identifying opportunities for process improvements, documenting technical processes and procedures, collaborating with other teams, and delivering training and development sessions.

## Hierarchical link



## Key interactions

Internally: Customers and users, Accor Senior Executives / ExComm, Other support teams, Other GSS excom and teams, HUB leaders

Externally: T4T Teams, Move 2 cloud team, T4H Teams, SDD (Service Delivery Directors)

## Main responsibilities

Senior IT Specialist plays a critical role in ensuring the smooth operation of an organization's network and server infrastructure. They are responsible for providing technical support, maintaining security, managing a team, and continuously improving the infrastructure to meet the needs of the organization..

- 1. Technical expertise:** The IT Senior Specialist is expected to have expert-level technical knowledge and experience in a particular area, such as network infrastructure, network, Accor applications, server or software.
- 2. Project management:** The IT Senior Specialist may be responsible for managing projects related to their area of expertise, including planning, execution, and monitoring of project activities.
- 3. Mentoring and coaching:** The IT Senior Specialist may be responsible for mentoring and coaching junior team members, sharing their technical knowledge and providing guidance and support.
- 4. Troubleshooting:** The IT Senior Specialist is responsible for troubleshooting complex technical issues that cannot be resolved by junior team members.
- 5. Continuous improvement:** The IT Senior Specialist is responsible for identifying opportunities for process improvements and implementing changes to increase efficiency and effectiveness.
- 6. Documentation:** The IT Senior Specialist is responsible for documenting technical processes and procedures, ensuring that knowledge is captured and shared across the organization.
- 7. Collaboration:** The IT Senior Specialist collaborates with other IT teams and stakeholders across the organization to ensure that technical solutions meet business requirements and are aligned with organizational goals.
- 8. Training and development:** The IT Senior Specialist may be responsible for organizing and delivering training sessions to junior team members or end-users to improve their technical knowledge and skills.
- 9. Escalation:** Senior specialist is responsible for documenting the troubleshooting steps and escalate to L3 or L4 depends on the support process.

## Main difficulties / Key Success factors related to the position

- Managing High complex incidents
- Language
- Understand the priority and deliver the service on within SLA
- Good customer service and communication skill

## Sizing : Turnover, budget, size of the teams, ...

- Worldwide scope
- Processes covering all Level 1 support
- Accor Tech Support perimeter
- Communication with the users and senior team
- Process management on 100K incidents

## Profile

### Educational background

- Minimum 6 years of experience in IT Support
- Experience in the hotel industry
- Process Management based on the ITIL framework
- Certifications in IT field particular area
- Experience in critical troubleshooting especially the particular job area

### Competencies

- Customer service skills
- Excellent English language skill
- Understanding of ITIL frame work
- Ability to effectively communicate with end users and other team members at varying levels
- Leadership skills

Job title

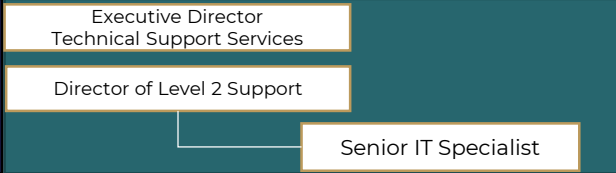
Senior IT Specialist – Tech Support Level 2 (Mandarin speaking)



Purpose

Senior Specialist plays a critical role in providing expert-level technical support, mentoring junior team members, managing projects, identifying opportunities for process improvements, documenting technical processes and procedures, collaborating with other teams, and delivering training and development sessions.

Hierarchical link



Key interactions

Internally: Customers and users, Accor Senior Executives / ExComm, Other support teams, Other GSS excom and teams, HUB leaders

Externally: T4T Teams, Move 2 cloud team, T4H Teams, SDD (Service Delivery Directors)

Main responsibilities

Senior IT Specialist plays a critical role in ensuring the smooth operation of an organization's network and server infrastructure. They are responsible for providing technical support, maintaining security, managing a team, and continuously improving the infrastructure to meet the needs of the organization..

- 1. Technical expertise:** The IT Senior Specialist is expected to have expert-level technical knowledge and experience in a particular area, such as network infrastructure, network, Accor applications, server or software.
- 2. Project management:** The IT Senior Specialist may be responsible for managing projects related to their area of expertise, including planning, execution, and monitoring of project activities.
- 3. Mentoring and coaching:** The IT Senior Specialist may be responsible for mentoring and coaching junior team members, sharing their technical knowledge and providing guidance and support.
- 4. Troubleshooting:** The IT Senior Specialist is responsible for troubleshooting complex technical issues that cannot be resolved by junior team members.
- 5. Continuous improvement:** The IT Senior Specialist is responsible for identifying opportunities for process improvements and implementing changes to increase efficiency and effectiveness.
- 6. Documentation:** The IT Senior Specialist is responsible for documenting technical processes and procedures, ensuring that knowledge is captured and shared across the organization.
- 7. Collaboration:** The IT Senior Specialist collaborates with other IT teams and stakeholders across the organization to ensure that technical solutions meet business requirements and are aligned with organizational goals.
- 8. Training and development:** The IT Senior Specialist may be responsible for organizing and delivering training sessions to junior team members or end-users to improve their technical knowledge and skills.
- 9. Escalation:** Senior specialist is responsible for documenting the troubleshooting steps and escalate to L3 or L4 depends on the support process.

Main difficulties / Key Success factors related to the position

- Managing High complex incidents
- Language
- Understand the priority and deliver the service on within SLA
- Good customer service and communication skill

Sizing : Turnover, budget, size of the teams, ...

- Worldwide scope
- Processes covering all Level 1 support
- Accor Tech Support perimeter
- Communication with the users and senior team
- Process management on 100K incidents

Profile

Educational background

- Minimum 6 years of experience in IT support
- Experience in the hotel industry
- Process Management based on the ITIL framework
- Certifications in IT field particular area
- Experience in critical troubleshooting especially the particular job area

Competencies

- Fluent in English language
- Fluent in Mandarin Language
- Customer service
- Excellent language skill
- Understanding of ITIL framework
- Ability to effectively communicate with end users and other team members at varying levels
- Leadership



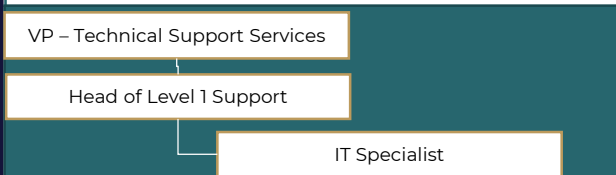
**Job title**

**IT Specialist – Tech Support Level 1**  
(German speaking)

**Purpose**

L1 IT Specialist plays a critical role in providing technical support and customer service to end-users, ensuring incidents and service requests are resolved efficiently and effectively, and contributing to the continuous improvement of the Service Desk function. They are responsible for documenting incidents and service requests, providing technical expertise, and working collaboratively with other members of the Service Desk team.

**Hierarchical link**



**Key interactions**

Internally: Customers and users, Accor Senior Executives / ExComm, Other support teams, Other GSS excom and teams, HUB leaders, T4T Teams, Move 2 cloud team, T4H Teams, SDD (Service Delivery Directors)

Externally:  
Vendors, partners & service providers

**Main responsibilities**

IT Specialist plays a critical role in providing technical support and customer service to end-users, ensuring incidents and service requests are resolved efficiently and effectively, and contributing to the continuous improvement of the Global Support Services function. They are responsible for documenting incidents and service requests, providing technical expertise, and working collaboratively with other members of the Global Support Services team.

**1. Providing technical support:** The primary responsibility of an L1 IT Specialist is to provide technical support to end-users. This includes troubleshooting technical issues, resolving incidents and service requests, and providing solutions to users.

**2. Incident management:** The L1 IT Specialist is responsible for logging incidents and service requests, prioritizing them based on impact and urgency, and ensuring that they are resolved within agreed service levels. This includes communicating with end-users throughout the incident lifecycle.

**3. Customer service:** The L1 IT Specialist is responsible for providing high-quality customer service at all times. This includes building relationships with end-users, understanding their needs, and resolving their technical issues efficiently and effectively. Use proper template for communication and achieve highest score in the customer satisfaction.

**4. Documentation:** The L1 IT Specialist is responsible for documenting all incidents and service requests, including the actions taken to resolve them. This documentation is critical to the knowledge management process and helps to ensure that technical issues can be resolved more quickly and effectively in the future.

**5. Continuous improvement:** The L1 IT Specialist is responsible for identifying opportunities for continuous improvement within the Global Support Services function. This includes providing feedback on processes and procedures, suggesting new tools or technologies, and contributing to knowledge management initiatives.

**6. Teamwork:** The L1 IT Specialist is expected to work collaboratively with other members of the Service Desk team, including L1 Team Leads, L2 Network and Server Senior Specialists, and Application Support Specialists, to resolve incidents and service requests and ensure high levels of customer satisfaction.

**Main difficulties / Key Success factors related to the position**

Troubleshooting skills  
Understand the priority and deliver the service on within SLA  
Good customer service and communication skill

**Sizing : Turnover, budget, size of the teams, ...**

- Worldwide scope
- Processes covering all Level 1 support
- Accor Tech Support perimeter
- Communication with the users
- Process management on 100K incidents

**Profile**

**Educational background**

- Minimum 3 years of experience in IT
- Experience in the hotel industry
- Process Management based on the ITIL framework
- Certifications in IT field

**Competencies**

- Customer service skills
- Excellent **English & German** language skill
- Understanding of ITIL frame work
- Ability to effectively communicate with end users and other team members at varying levels

2

*Security*





**Job title**

**Director, IT Security Infrastructure**



**Purpose**

Accor is a dynamic and innovative hospitality company committed to excellence for our customers, hotels owners and our employees. To succeed in this mission, we are seeking a highly skilled and experienced IT Security Infrastructure Director to join our cyber security team and lead our efforts in maintaining a secure and resilient IT environment.

**Hierarchical link**

Senior VP Security - CISO

Director, Information Security Infrastructure

**Key interactions**

Strategic planning & Leadership of Information Security Infrastructure team

Conduct Risk Management and implement security controls

**Main responsibilities**

**Profile**

**Strategic Planning:**

- Develop and implement the overall IT security infrastructure strategy aligned with organizational objectives.
- Provide expertise in designing, implementing, and maintaining security measures for the organization's IT infrastructure.

**Leadership:**

- Lead and mentor a team of IT security professionals, fostering a culture of continuous learning and development.
- Collaborate with cross-functional teams to integrate security measures into various IT projects.

**Risk Management:**

- Identify, assess, and prioritize security risks, and develop strategies to mitigate potential threats.
- Implement and manage a robust incident response and recovery plan.

**Infrastructure Security:**

- Oversee the design, deployment, and maintenance of secure network architecture.
- Implement and manage security controls for servers, databases, and other critical IT assets (on premise and in the cloud).

**Compliance:**

- Ensure compliance with industry regulations and standards related to IT security.
- Collaborate with internal and external auditors to conduct regular security assessments.

**Educational background**

- Bachelor's or master's degree in information technology, Cybersecurity, or a related field.
- Proven experience (10+ years) in a leadership role within IT security infrastructure.
- In-depth knowledge of cybersecurity principles, technologies, and best practices.
- Industry certifications such as CISSP, CISM, or similar are highly desirable.
- Have a palatability for IaaS/PaaS technologies

**Competencies**

- Strong leadership and team management skills.
- Excellent communication and interpersonal abilities.
- Deep understanding of network security, encryption, and vulnerability management.
- Proficient in evaluating and implementing security technologies.

## Job title

# Cloud Security Engineer



## Purpose

As a Cloud Security Engineer, your primary mission is to secure our organization's Cloud Service Providers while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions as well as secure architectures for the whole Accor group. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment. This position offers dynamic career progression through continuous training, role evolution, and expanding responsibilities.

## Hierarchical link

Infrastructure Director

Cloud Security Engineer

## Key interactions

Work closely with SMEs to enforce a good security level worldwide.

Provide on-demand security expertise for the whole group

## Main responsibilities

### 1. Design:

- Collaborate with internal technical teams, customers, and external strategic partners to define, deliver and improve high-quality secure architectures for all our CSPs.
- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

### 2. Implement and Manage:

- Install, configure, and maintain security solutions and tools to ensure a secure usage of CSPs.
- Maintain the procedures for these tools.
- Implement and develop a Policy-as-Code approach.

### 3. Expertise & transversal:

- Provide timely subject matter expertise for incidents and requests related to cloud security.
- Assist the whole team on other subjects and tools related to Cyber Security.
- Stay up to date with emerging security threats, vulnerabilities, and technologies.
- Advise on and enforce the Security policies across the group.

## Profile

### Educational Background

- At least a 5-year university degree in technology.
- At least 5 years as a cloud security engineer or architect (if run activities where part of the position), or cloud engineer - with hands on experience in security solutions and practices.
- Security industry certifications and/or security vendors specific trainings are a plus.

### Competencies

#### Required Technical Skills and Knowledge:

- Mandatory Knowledge of Azure, GCP and OCI
- Mandatory experience of DevSecOps practices & tools (Vault, Gitlab / Gitlab CI, Terraform, Ansible).
- Experience with CNAPP / CSPM tools such as Cloudguard , Prisma Cloud, Trivy.
- Intermediate skills in programming language (python).
- Strong knowledge of security protocols and principles.
- Knowledge of security systems, including firewalls, EPP and EDR, content filtering, authentication systems, and reverse proxies, SIEM

#### Soft Skills:

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Cloud Security Engineer, AWS



## Purpose

As a Cloud Security Engineer, your primary mission is to secure our organization's Cloud Service Providers while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions as well as secure architectures for the whole Accor group. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment

## Hierarchical link

Infrastructure Security & SOC manager

Cloud Security Engineer

## Key interactions

Work closely with the whole security team to enforce a good security level

Provide on-demand security expertise for the whole group

## Main responsibilities

## Profile

### 1. Design:

- Collaborate with internal technical teams, customers, and external strategic partners to define, deliver and improve high-quality secure architectures for all our CSPs.
- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

### 2. Implement and Manage:

- Install, configure, and maintain security solutions and tools to ensure a secure usage of CSPs.
- Maintain the procedures for these tools.
- Implement and develop a Policy-as-Code approach.

### 3. Expertise & transversal:

- Provide timely subject matter expertise for incidents and requests related to cloud security.
- Assist the whole team on other subjects and tools related to Cyber Security.
- Stay up to date with emerging security threats, vulnerabilities, and technologies.
- Advise on and enforce the Security policies across the group.

## Educational Background

- At least a 5-year university degree in technology.
- At least 5 years as a cloud security engineer or architect (if run activities where part of the position), or cloud engineer - with hands on experience in security solutions and practices.
- Security industry certifications and/or security vendors specific trainings are a plus.

## Competencies

### Required Technical Skills and Knowledge:

- Mandatory experience with AWS.
- Mandatory experience of DevSecOps practices & tools (Vault, Gitlab / Gitlab CI, Terraform, Ansible).
- Experience with CNAPP / CSPM tools such as Cloudguard , Prisma Cloud, Trivy.
- Intermediate skills in programming language (python).
- Strong knowledge of security protocols and principles.
- Knowledge of security systems, including firewalls, EPP and EDR, content filtering, authentication systems, and reverse proxies, SIEM

### Soft Skills:

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Cloud Security Engineer, Azure



## Purpose

As a Cloud Security Engineer, your primary mission is to secure our organization's Cloud Service Providers while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions as well as secure architectures for the whole Accor group. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment

## Hierarchical link



## Key interactions

- Work closely with the whole security team to enforce a good security level
- Provide on-demand security expertise for the whole group

## Main responsibilities

## Profile

- 1. Design:**
  - Collaborate with internal technical teams, customers, and external strategic partners to define, deliver and improve high-quality secure architectures for all our CSPs.
  - Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.
- 2. Implement and Manage:**
  - Install, configure, and maintain security solutions and tools to ensure a secure usage of CSPs.
  - Maintain the procedures for these tools.
  - Implement and develop a Policy-as-Code approach.
- 3. Expertise & transversal:**
  - Provide timely subject matter expertise for incidents and requests related to cloud security.
  - Assist the whole team on other subjects and tools related to Cyber Security.
  - Stay up to date with emerging security threats, vulnerabilities, and technologies.
  - Advise on and enforce the Security policies across the group.

### Educational Background

- At least a 5-year university degree in technology.
- At least 5 years as a cloud security engineer or architect (if run activities where part of the position), or cloud engineer - with hands on experience in security solutions and practices.
- Security industry certifications and/or security vendors specific trainings are a plus.

### Competencies

- Required Technical Skills and Knowledge:**
- Mandatory experience with Azure and, Azure AD authentication and authorizations mechanisms.
  - Mandatory experience of DevSecOps practices & tools (Vault, Gitlab / Gitlab CI, Terraform, Ansible).
  - Experience with CNAPP / CSPM tools such as Cloudguard , Prisma Cloud, Trivy.
  - Intermediate skills in programmation language (python).
  - Strong knowledge of security protocols and principles.
  - Knowledge of security systems, including firewalls, EPP and EDR, content filtering, authentication systems, and reverse proxies, SIEM
- Soft Skills:**
- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
  - Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
  - Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
  - Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
  - Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Security Analyst SOC



## Purpose

As a Security Analyst, your primary mission will be to protect our organization's information systems, data, and applications by responding to threats, conducting in-depth threat analysis, providing expertise on how to handle such threats, improving the SOC capabilities and its seamless integration within the Information System. You will play a critical role in mitigating vulnerabilities and attacks, identifying potential security risks, and continuously improving our security posture.

## Hierarchical link

Infrastructure Security & SOC manager

Security Analyst SOC

## Key interactions

Respond to threats for the whole Information System

Coordinate with all stakeholders to improve the Protect, Detect and React capabilities of the Cyber Security team

## Main responsibilities

## Profil

**1. All members of the SOC team are expected to be able to respond to security incidents promptly, investigate breaches, and implement measures to prevent future occurrences.**

### 2. Analyze and respond to threats:

- Monitor threats (TTPs, threat actor groups, ...) and maintain a threat landscape for the Information System.
- Build and manage the lifecycle of the SOC playbooks and processes.
- Respond to alerts coming from our managed services or directly from our tools.
- Perform incident response and forensics.
- Assist the SOC manager in coordinating alerts and incidents handling with all stakeholders and partners.
- Conduct regular Threat Hunting activities and develop a threat hunting program.

### 3. Expertise & transversal:

- Assist the team in implementing a detection engineering methodology.
- Assist the whole team on other subjects and tools related to Cyber Security.
- Advise on and enforce the Security policies across the group.
- Assist the Vulnerability engineers to proactively identify and address potential weaknesses.
- Help developing a purple team activity with the offensive security team.

## Educational Background

- At least a 2-year university degree in technology.
- At least 3 years as a security analyst in SOC with hands on experience in a blue team.
- Security industry certifications and/or security vendors specific trainings are a plus.

## Competencies

### Required Technical Skills and Knowledge:

- Mandatory experience with SIEM, and alerts from proxies, email gateways and EPP/EDR.
- Mandatory experience in log and alerts analysis, threat hunting and incident response methodologies.
- Strong knowledge of networking technologies, network security, and monitoring principles.
- In-depth knowledge of security protocols and principles.
- Knowledge of cloud security principles (especially for AWS or Azure).
- Proficiency in various operating systems (e.g., Windows, Linux, Unix) and cloud environments.
- Experience in scripting.

### Soft Skills:

- Ability to analyze complex issues and quickly devise effective solutions fitting the business context or risk. Attention to details.
- Excellent communication skills to convey technical information to both technical and non-technical stakeholders. Ability to handle working under stress for critical security incidents.
- Able to stay updated with rapidly evolving security threats and adjust security strategies accordingly.
- Strong teamwork and collaboration skills to work effectively across departments.
- A strong sense of ethics and responsibility in handling sensitive data and security matters.
- Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Security Analyst Junior SOC



## Purpose

As a Security Analyst, your primary mission will be to protect our organization's information systems, data, and applications by responding to threats, conducting in-depth threat analysis, providing expertise on how to handle such threats, improving the SOC capabilities and its seamless integration within the Information System. You will play a critical role in mitigating vulnerabilities and attacks, identifying potential security risks, and continuously improving our security posture.

## Hierarchical link

Infrastructure Security & SOC manager

Security Analyst junior SOC

## Key interactions

Respond to threats for the whole Information System

Coordinate with all stakeholders to improve the Protect, Detect and React capabilities of the Cyber Security team

## Main responsibilities

### 1. Manage security alerts and incidents:

- Respond to alerts coming from our managed services or directly from our tools: triage, analysis and investigation, containment and remediation.
- Perform these investigations across all our tools.
- Assist the SOC members in coordinating alerts and incidents handling with all stakeholders and partners.
- Assist in incident response and forensics.

### 2. Expertise & transversal:

- Assist in building and managing the lifecycle of the SOC playbooks and processes.
- Assist the team in implementing a detection engineering methodology.
- Assist the Vulnerability engineers to proactively identify and address potential weaknesses.

## Profile

### Educational Background

- At least a 2-year university degree in technology.
- At least 2 years as a security analyst in SOC with hands on experience in a blue team.
- Security industry certifications and/or security vendors specific trainings are a plus.

### Competencies

#### Required Technical Skills and Knowledge:

- Mandatory experience with SIEM, and alerts from proxies, email gateways and EPP/EDR.
- Mandatory experience in log and alerts analysis and incident response methodologies.
- Strong knowledge of networking technologies, network security, and monitoring principles.
- Good knowledge of security protocols and principles.
- Knowledge in various operating systems (e.g., Windows, Linux, Unix) and cloud environments.

#### Soft Skills:

- Ability to analyze complex issues and quickly devise effective solutions fitting the business context or risk. Attention to details.
- Excellent communication skills to convey technical information to both technical and non-technical stakeholders. Ability to handle working under stress for critical security incidents.
- Able to stay updated with rapidly evolving security threats and adjust security strategies accordingly.
- Strong teamwork and collaboration skills to work effectively across departments.
- A strong sense of ethics and responsibility in handling sensitive data and security matters.
- Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Security Engineer (IT tools)



## Purpose

As a specialist in the security engineer of SaaS and enterprise solutions, your main mission is to secure third-party SaaS solutions as well as IT tools used at the enterprise level (O365, SAP, etc.) throughout our organization. Keeping the business operational. You will lead efforts to ensure that integrated external tools comply with security policies at Accor. By working closely with technical teams, you will improve our security posture and you will be responsible for ensuring that the security level of third-party solutions is maintained and ensure a resilient and secure environment. This position offers dynamic career progression through continuing education, role development and expanded responsibilities.

## Hierarchical link

Security Infrastructure Director

Security Engineer (SaaS & Corporate tools )

## Key interactions

Work closely with SMEs to enforce a good security level worldwide

Provide on-demand security expertise for the whole group

## Main responsibilities

### 1. Study:

- Evaluate the security of third-parties solutions at Accor based on internal framework.
- Manage the security of O365 office solutions.
- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

### 2. Validate:

- Validate the security requirements of third parties solutions for IT, corporate and Business.
- Setup and follow security processes and governance for the operating of these tools.

### 3. Monitor & remediate:

- Provide timely subject matter expertise for the security of third-parties solutions.
- Assist the whole team on other subjects and tools related to Cyber Security.
- Stay up to date with emerging security threats, vulnerabilities, and technologies.

## Profile

### Educational Background

- At least a 5-year university degree in technology.
- At least 3 years as a cloud security engineer or architect (if run activities where part of the position), or cloud engineer - with hands on experience in security solutions and practices.
- Security industry certifications and/or security vendors specific trainings are a plus.

### Competencies

#### Required Technical Skills and Knowledge:

- Mandatory experience with SaaS cloud services providers .
- Mandatory experience of DevSecOps practices & tools (Vault, Gitlab / Gitlab CI, Terraform, Ansible).
- Experience Microsoft O365, endpoint security.
- Intermediate skills in programming language (python).
- Strong knowledge of security protocols and principles.
- Knowledge of security standards ( SOC2, GDPR .. ) and strong ability to analyze and identify risks and remediations

#### Soft Skills:

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Security Engineer SOC



## Purpose

As a Security Engineer, your primary mission will be to protect our organization's information systems, data, and applications by implementing robust security measures (Protect), deploying Detect and React workflows, conducting in-depth threat analysis, as well as ensuring seamless integration of security practices within the Information System. You will play a critical role in identifying potential security risks, mitigating vulnerabilities and attacks, and continuously improving our security posture.

## Hierarchical link



## Key interactions

Pilot the threat response automation initiative for the whole Information System

Coordinate and implement (Dev)SecOps practices with all stakeholders

## Main responsibilities

- All members of the SOC team are expected to be able to respond to security incidents promptly, investigate breaches, and implement measures to prevent future occurrences.**
- Design, implement and manage detection and response tools:**
  - Develop and implement a detection engineering methodology, with code and pipelines.
  - Develop and deploy security solutions to monitor systems, applications, and networks against cyber threats, malware, unauthorized access...
  - Monitor threats (TTPs, threat actor groups, ...) and maintain a threat landscape for the Information System. Build and manage the lifecycle of the associated SOC playbooks.
  - Develop Detection and Response automation capabilities.
  - Maintain the tools and document their usage.
- Expertise & transversal:**
  - Write Detection and Response processes and playbooks according to threats & tools.
  - Assist the whole team on other subjects and tools related to Cyber Security.
  - Advise on and enforce the Security policies across the group.
  - Assist the Vulnerability engineers to proactively identify and address potential weaknesses.
  - Help developing a purple team activity with the offensive security team.

## Profile

### Educational Background

- At least a 2-year university degree in technology.
- At least 5 years as a security engineer in SOC with hands on experience in security solutions (SIEM and/or SOAR).
- Security industry certifications and/or security vendors specific trainings are a plus.

### Competencies

#### Required Technical Skills and Knowledge:

- Mandatory experience with Splunk. Experience with SOAR tools.
- Strong knowledge of networking technologies, network security, and monitoring principles.
- In-depth knowledge of security protocols and principles.
- Experience in log analysis and security event monitoring, alerts analysis and incident response methodologies.
- Knowledge of cloud security principles (especially for AWS or Azure).
- Proficiency in various operating systems (e.g., Windows, Linux, Unix) and cloud environments.
- Experience in scripting. Knowledge of DevSecOps approaches

#### Soft Skills:

- Ability to analyze complex issues and quickly devise effective solutions fitting the business context or risk. Attention to details.
- Excellent communication skills to convey technical information to both technical and non-technical stakeholders. Ability to handle working under stress for critical security incidents.
- Able to stay updated with rapidly evolving security threats and adjust security strategies accordingly.
- Strong teamwork and collaboration skills to work effectively across departments.
- A strong sense of ethics and responsibility in handling sensitive data and security matters.
- Eagerness to stay updated with the latest security trends and technologies.



## Job title

# Security Engineer, Expert Firewall



## Purpose

As a Security Engineer, specializing in firewalls, your primary mission is to fortify our organization's cybersecurity defenses while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions for the whole Accor group. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment

## Hierarchical link

Infrastructure Security manager

Security Engineer (Expert Firewall)

## Key interactions

Work closely with the whole security team to enforce a good security level

Provide security expertise to other BUs to Accor group

## Main responsibilities

## Profile

### 1. Implement, Manage, Maintain:

- Install, configure, and maintain network infrastructure tools (firewalls), to ensure a secure and reliable access to corporate resources while following the security policies.
- Implement configuration changes.
- Provide timely subject matter expertise for incidents and requests related to remote access tools.
- Maintain the procedures for these tools.

### 2. Expertise & transversal:

- Collaborate with internal technical teams, customers, and external strategic partners to deliver and improve high-quality secure networks supporting Accor's global Information System.
- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

## Educational Background

- Bachelor's degree or higher in technology field.
- At least 5 years as a security engineer or architect (if run activities where part of the position), or network engineer - with hands on experience in security solutions.
- Security industry certifications and/or security vendors specific trainings are a plus.

## Competencies

### Required Technical Skills and Knowledge:

- Mandatory experience with **Checkpoint**.
- Mandatory experience with **Tufin**.
- Experience with Forcepoint.
- Strong knowledge of networking technologies, network security, and network monitoring solutions as well as Zero Trust approach.
- In-depth knowledge of security protocols and principles.
- Knowledge of cloud security principles, such as AWS or Azure.
- Knowledge of security systems, including EPP and EDR, content filtering, authentication systems, and reverse proxies.

### Soft Skills:

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Security Engineer, Firewall Manager



## Purpose

As a Security Engineer, specializing in firewalls, your primary mission is to fortify our organization's cybersecurity defenses while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions for the whole Accor group. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment

## Hierarchical link

Infrastructure Security & SOC manager

Security Engineer, Firewall

## Key interactions

Work closely with the whole security team to enforce a good security level

Provide on-demand security expertise for the whole group

## Main responsibilities

## Profile

### 1. Design:

- Collaborate with internal technical teams, customers, and external strategic partners to define, deliver and improve high-quality network segmentation for all Accor's hotels and the hotel standard
- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

### 2. Act as a L3 engineer:

- Install, configure, and maintain firewalls and network security devices, to ensure a secure and reliable access to corporate resources while following the security standard.
- Provide timely subject matter expertise for incidents and requests related to network security.
- Maintain the procedures for these tools.

### 3. Expertise & transversal:

- Coordinate with the MSSP in charge of the hotels' firewall
- Assist the whole team on other subjects and tools related to Cyber Security.
- Stay up to date with emerging security threats, vulnerabilities, and technologies.
- Advise on and enforce the Security policies across the group.

## Educational Background

- At least a 2-year university degree in technology.
- At least 5 years as a security engineer or architect (if run activities where part of the position), or network engineer - with hands on experience in security solutions.
- Security industry certifications and/or security vendors specific trainings are a plus.

## Competencies

### Required Technical Skills and Knowledge:

- Mandatory experience with Forcepoint.
- Experience with Checkpoint, Pulse Secure, Zscaler Internet Access and/or Zscaler Private Access is a plus.
- Strong knowledge of networking technologies, network security, and network monitoring solutions.
- In-depth knowledge of security protocols and principles.
- Knowledge of cloud security principles, such as AWS or Azure.
- Knowledge of security systems, including EPP and EDR, content filtering, authentication systems, and reverse proxies.

### Soft Skills:

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

**Job title**

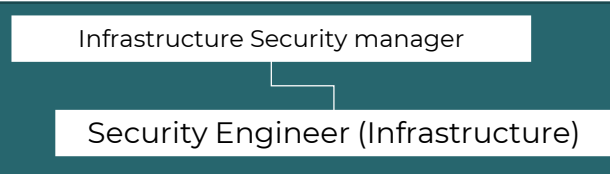
**Security Engineer, Infrastructure**



**Purpose**

As a Security Engineer, specializing in infrastructure, your primary mission is to fortify our organization's cybersecurity defenses while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions for the whole Accor group. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment

**Hierarchical link**



**Key interactions**

Work closely with the whole security team to enforce a good security level

Provide security expertise to other BUs to Accor group

**Main responsibilities**

**Profile**

**1. Implement, Manage, Maintain:**

- Install, configure, and maintain network infrastructure tools (reverse-proxies, network load balancers, firewalls...), to ensure a secure and reliable access to corporate resources while following the security policies.

- Implement configuration changes.

- Provide timely subject matter expertise for incidents and requests related to remote access tools.

- Maintain the procedures for these tools.

**2. Expertise & transversal:**

- Collaborate with internal technical teams, customers, and external strategic partners to deliver and improve high-quality secure networks supporting Accor's global Information System.

- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

**Educational Background**

- Bachelor's degree or higher in technology field.
- At least 5 years as a security engineer or architect (if run activities where part of the position), or network engineer - with hands on experience in security solutions.
- Security industry certifications and/or security vendors specific trainings are a plus.

**Competencies**

**Required Technical Skills and Knowledge:**

- Mandatory experience with **Imperva**.
- Experience with Checkpoint, Forcepoint, F5, Tufin is a plus.
- Strong knowledge of networking technologies, network security, and network monitoring solutions as well as Zero Trust approach.
- In-depth knowledge of security protocols and principles.
- Knowledge of cloud security principles, such as AWS or Azure.
- Knowledge of security systems, including EPP and EDR, content filtering, authentication systems, and reverse proxies.

**Soft Skills:**

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

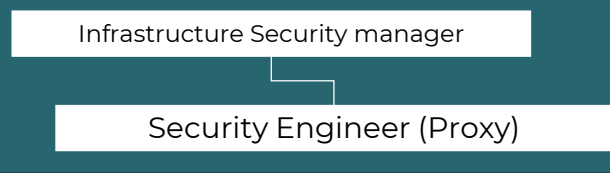
# Security Engineer, Proxy



## Purpose

As a Security Engineer, specializing in proxy and reverse proxies, your primary mission is to fortify our organization's cybersecurity defenses while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions for the whole Accor group. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment

## Hierarchical link



## Key interactions

Work closely with the whole security team to enforce a good security level

Provide security expertise to other BUs to Accor group

## Main responsibilities

### 1. Implement, Manage, Maintain:

- Install, configure, and maintain network infrastructure tools (proxies and reverse-proxies), to ensure a secure and reliable access to corporate resources while following the security policies.

- Implement configuration changes.

- Provide timely subject matter expertise for incidents and requests related to remote access tools.

- Maintain the procedures for these tools.

### 2. Expertise & transversal:

- Collaborate with internal technical teams, customers, and external strategic partners to deliver and improve high-quality secure networks supporting Accor's global Information System.

- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

## Profile

### Educational Background

- Bachelor's degree or higher in technology field.
- At least 5 years as a security engineer or architect (if run activities where part of the position), or network engineer - with hands on experience in security solutions.
- Security industry certifications and/or security vendors specific trainings are a plus.

### Competencies

#### Required Technical Skills and Knowledge:

- Mandatory experience with **Zscaler, McAfee**,
- Mandatory experience with Imperva, **F5**.
- Strong knowledge of networking technologies, network security, and network monitoring solutions as well as Zero Trust approach.
- In-depth knowledge of security protocols and principles.
- Knowledge of cloud security principles, such as AWS or Azure.
- Knowledge of security systems, including EPP and EDR, content filtering, authentication systems, and reverse proxies.

#### Soft Skills:

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Security Engineer, Remote Access Specialization



## Purpose

As a Security Engineer, specializing in remote access solutions, your primary mission is to fortify our organization's cybersecurity defenses while maintaining the business up and running. You will lead efforts to design, implement and manage robust security solutions to protect our critical assets. Collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure environment

## Hierarchical link

Infrastructure Security & SOC manager

Security Engineer, RA

## Key interactions

Work closely with the whole security team to enforce a good security level

Provide security expertise to other BUs in Accor

## Main responsibilities

## Profile

### 1. Design:

- Collaborate with internal technical teams, customers, and external strategic partners to deliver and improve high-quality secure systems providing remote accesses to Accor's Information System.

- Engage with the whole Cyber Security team to develop security policies, protocols, and procedures.

### 2. Implement and Manage:

- Install, configure, and maintain remote access tools, to ensure a secure and reliable access to corporate resources while following the security policies.

- Provide timely subject matter expertise for incidents and requests related to remote access tools.

- Maintain the procedures for these tools.

### 3. Expertise & transversal:

- Provide timely subject matter expertise for critical security incidents related to remote access tools.

- Assist the whole team on other subjects and tools related to Cyber Security.

- Stay up to date with emerging security threats, vulnerabilities, and technologies.

- Advise on and enforce the Security policies across the group.

## Educational Background

- At least a 2-year university degree in technology.
- At least 5 years as a security engineer or architect (if run activities where part of the position), or network engineer - with hands on experience in security solutions.
- Security industry certifications and/or security vendors specific trainings are a plus.

## Competencies

### Required Technical Skills and Knowledge:

- Mandatory experience with Zscaler Private Access.
- Experience with Pulse Secure and/or Bomgar is a plus.
- Strong knowledge of networking technologies, network security, and network monitoring solutions as well as Zero Trust approach.
- In-depth knowledge of security protocols and principles.
- Knowledge of cloud security principles, such as AWS or Azure.
- Knowledge of security systems, including EPP and EDR, content filtering, authentication systems, and reverse proxies.

### Soft Skills:

- Analytical Thinking: Ability to analyze complex issues and quickly devise effective solutions fitting the business context. Attention to details.
- Communication: Excellent communication skills to convey technical information to both technical and non-technical stakeholders.
- Proactive Approach: A problem-solving mindset with a proactive approach to identify and address security challenges.
- Collaboration: Strong teamwork and collaboration skills to work effectively across departments.
- Continuous Learning: Eagerness to stay updated with the latest security trends and technologies.

## Job title

# Vulnerability Management Officer



## Purpose

As a Vulnerability Management Officer, your primary mission will be to implement a governance on vulnerability management. You will also lead the management of the build and run of the vulnerability tools. You will be collaborating closely with cross-functional teams, you will enhance our security posture and ensure a resilient and secure information system. This position offers dynamic career progression through continuous training, role evolution, and expanding responsibilities.

## Hierarchical link



## Key interactions

Work closely with Subject Matter Experts to enforce a good security level worldwide

Provide security expertise to other BUs to Accor group

## Main responsibilities

## Profile

### 1. Implement, Manage, Maintain:

- Be the expert (build and run) of the main vulnerability scanning tool
- Implement and regularly review scheduled scans, perimeters, roles and accesses...
- Define the right scanning methodologies & tools according to the needs (agent/agentless/On-Prem/laaS/external/...)
- Automate recurring tasks (Management of network ranges to be scanned / Management and follow-up of remediations via our SNow ticketing tool / etc...)

### 2. Vulnerabilities governance:

- Review and adapt the organizational model, roles and responsibilities, scopes to fit Accor operating model
- Provide KPIs to and follow up vulnerabilities with all stakeholders
- Identify, initiate and coordinate remediation efforts for scopes outside of Cybersecurity's direct responsibility

### 3. Expertise & transversal:

- Collaborate with internal technical teams, customers, and external strategic partners to have a holistic and coherent vulnerability management approach.
- Engage with the whole Cyber Security team to enhance their practices (help prioritizing new use cases for the SOC, monitor vulnerabilities for our technical scope...)

## Educational Background

- At least a 2-year university degree in technology.
- At least 3 years as a security analyst, with hands on experience in Vulnerability management.
- Security industry certifications and/or security vendors specific trainings are a plus.

## Competencies

### Required Technical Skills and Knowledge:

- Mandatory experience with Qualys cloud (inc. VMDR) and Qualys agents.
- Strong knowledge of Vulnerability Management processes
- Knowledge of SOC tools and processes
- Experience with programming languages like Python
- Knowledge of security systems, including EPP and EDR, content filtering, authentication systems, and reverse proxies and their usefulness

### Soft Skills:

- Ability to analyze complex issues and quickly devise effective solutions fitting the business context or risk. Attention to details.
- Excellent communication skills to convey technical information to both technical and non-technical stakeholders. Ability to handle working under stress for critical security incidents.
- Able to stay updated with rapidly evolving security threats and adjust security strategies accordingly.
- Strong teamwork and collaboration skills to work effectively across departments.
- A strong sense of ethics and responsibility in handling sensitive data and security matters.
- Eagerness to stay updated with the latest security trends and technologies.

3

# *Infrastructure & Operations*



**Job title**

**DevOps Engineer**



**Purpose**

Drive the construction, evolution, and maintenance of our Software Factory platform and empower our teams by providing guidance and support for its effective utilization.

**Hierarchical link**

Software Factory Lead

DevOps Engineer

**Key interactions**

Development and Operations Teams: monitor incident  
Operations team: interface with change management and other tools  
Security team: PCI DSS compliance

**Main responsibilities**

**Main difficulties / Key Success factors related to the position**

**Responsibilities and Activities:**

- Contribute to the construction and maintenance of the Software Factory platform
- Assist and train project teams in setting up CI/CD (continuous integration and deployment) chains
- Develop expertise and keep up-to-date with DevSecOps topics
- Innovate by proposing new ideas and demonstrating initiative
- Participate in the animation and sharing of experience through demonstrations, retrospectives, feedback, etc,
- Contribute to the writing and maintenance of platform documentation: user guide, onboarding guide, operation guide
- Systematically take into account FinOps aspects

**Certifications:**

AWS Certified Solution Architect Associate (Required)  
Certified Kubernetes Application Developer (optional)  
GitLab DevOps Professional Certificate (optional)

**Required skills:**

Software Architect  
Software Craftmanship (java or nodejs or golang)  
CI/CD Expert  
Gitlab, Ansible, Terraform, Helm  
Security OWASP Top 10

**Technical context around the platform:**

Jira/Confluence, ServiceNow, SonarQube, Nexus, Checkmarx, Splunk, Dynatrace, Neoload, SoapUI

- Collaborate with development teams to design and implement scalable and reliable software systems.
- Automate the deployment, monitoring, and maintenance of applications and infrastructure.
- Identify and troubleshoot issues in the production environment and implement effective solutions.
- Continuously improve processes and practices to enhance the reliability and performance of our systems.

**Sizing : Turnover, budget, size of the teams, ...**

- Not Applicable

**Profile**

**Educational background**

- Bachelor's or Master's degree in Computer Science or Engineering
- At least 3-5 years of experience in a DevOps role.
- Strong understanding of cloud computing technologies.

**Competencies**

- AWS: EKS, RDS, NLB, ElastiCache, OpenSearch, Lambda, IAM, SSM Agent, Kubernetes, prometheus, kibana, alert-manager, thanos, external-dns, nginx-ingress, fluentd, descheduler, pod-reaper, Hashicorp Vault
- GitLab CI, Terraform, helm, ansible, nexus.
- pipelines Maven, Npm, Python, AWS Lambda
- pipelines Terraform et Ansible, configuration de GitLab "as Code"
- Checkmarx, Checkov, trivy, GitLeaks



**Job title**

**Performance Engineer**



**Purpose**

Responsible for overseeing the implementation and maintenance of performance measurement tools. Provide support and guidance to teams to execute performance tests.

**Hierarchical link**

Method/Performance, Observability & Supervision Manager

Performance Engineer

**Key interactions**

Development and Operations Teams: evolve the platform according to their needs.

Operations team: interface with change management and other tools.  
Security team: PCI DSS compliance.

**Main responsibilities**

**Main difficulties / Key Success factors related to the position**

**Responsibilities and Activities:**

- Implementation and operational maintenance of performance measurement tools
- Proposing alternative or complementary solutions and contributing to the performance strategy with the tech lead
- Ensuring product and technical upgrades
- Providing support and guidance to teams in scripting, executing tests, and analyzing results
- Contributing to the automation of performance tests through the software factory
- Documentation: user guides, onboarding materials, and operational manuals.

**Technical environment:**

- Neoload
- Ready API : Service V
- Gitlab CI/ Automatisation
- AWS
- Linux
- Dynatrace
- Jira/Confluence

- Ability to develop and run a comprehensive performance test
- Ability to develop and run mocks for api
- Strong analytical skills and attention to detail to identify and troubleshoot performance issues
- Collaborative mindset and ability to work effectively with cross-functional teams, including developers, testers, and operations

**Sizing : Turnover, budget, size of the teams, ...**

- Not Applicable

**Profile**

**Educational background**

- Bachelor's or Master's degree in Computer Science, Software Engineering or a related field
- At least 3-5 years of experience in a similar role
- Neoload certification

**Competencies**

- Neoload
- ReadyApi Service V
- Gitlab CI / Automatisation
- AWS
- Linux

**Job title**

**Cloud Engineer**

NOV  
2023



**Purpose**

Responsible for implementing, maintaining, optimizing, and troubleshooting cloud-based systems, with a focus on AWS and DevOps principles.

**Hierarchical link**

Deputy Head of Cloud Platform

Cloud Engineer

**Key interactions**

Cloud teams, Enterprise Architecture, Operations, Security

Development teams, Application and Product owners

**Main responsibilities**

**Main difficulties / Key Success factors related to the position**

- Implementing, maintaining, and troubleshooting cloud-based systems.
- Ensuring that cloud-based systems are secure, reliable and scalable.
- Implementing cloud-based systems and services according to design specifications provided by the Cloud Architect. Work collaboratively with Architecture and other teams to participate in the definition of the Accor technical standards.
- Implementing solutions to automate deployments of system components.
- Managing and monitoring cloud-based systems and services.
- Participating in incident management and maintenance of incident reports.
- Collaborating with other teams and departments to identify and resolve cloud-related problems and optimize cloud performance.
- Work with the FinOps team to implement the cost optimization strategy.
- Continuously researching and staying up-to-date on new technologies and best practices in cloud computing.
- Managing and maintaining cloud-related documentation.
- Participating in the design, development and delivery of Continuous Integration/Continuous Deployment (CI/CD) pipeline.
- Effective communication skills (written and verbal) to properly document implementations steps, code, document to support the solution, incidents

- Adoption of these new practices.
- Acceleration of the development of expertise.
- Automation and industrialization of deployments.
- Standardization and dissemination of best practices.
- Rigor in interventions to avoid compromising the availability of services.

**Sizing : Turnover, budget, size of the teams, ...**

- No management responsibilities

**Profile**

**Educational background**

- Master in Computer Science
- Minimum 5+ years of experience on AWS
- DevOps Cloud
- Experience with Agile framework
- English Fluent

**Competencies**

- Strong hands-on experience with AWS and DevOps principles.
- Strong experience in cloud infrastructure management and troubleshooting.
- Strong understanding of cloud security and data management best practices.
- Experience with CI/CD pipeline and tooling Ansible, Terraform for 2+ years; Gitlab-CI; Containers (ECS, Fargate, K8S).
- Positive attitude and a strong commitment to delivering quality work

4

# *Tech for Accor teams*



## Job title

# Identity Engineer (Digital workplace)



## Purpose

Maintain, Secure and Develop the identity infrastructure of Accor

## Hierarchical link

Head of Digital Workplace

DW Identity Engineer

## Key interactions

Internally: Digital Workplace Team

Externally: L3 Digital Workplace support team (India)

## Main responsibilities

The Digital Workplace Identity team **manage incidents and requests that the L3 support teams can't handle**. This requires a strong level of skills in Microsoft technologies (Active Directory, EntraID, Microsoft365, ADConnect Cloud Sync, Powershell, SCOM, etc.) and analytical mindset.

You will also assist the TechLeads to follow security best practices (PingCastle, TenableAD, ForestDruid, PurpleKnight) and maintain a Tier0 security.

Fluency in technical English (written and oral) and French is welcome.

You will work in pairs with passionate experts in France (regular trip possible).

The team is also working on several projects like Merge&Aquisition projects, IAM/IGA implementation and continuous improvement with regards to PCIDSS.

### Main missions:

Active Directory/DNS:

Responsible for AD and DNS infrastructure, hardening, automations, monitoring

Azure AD / Entra ID:

Responsible for EntraID/M365 security, automation

(LogicApp/AzureAutomation/Runbook/...), standardization, monitoring.

Other identity infrastructures:

ADFS, MIM, PingIdentity, Quest ActiveRole

### Mandatory Skills

Expert on AD and DNS (L3 minimum)

Expert on PowerShell

AzureAD/EntraID: Good knowledge of all aspects related to Entra ID

(Enterprise App/App Registration/Conditional Access/MFA) As well as the

features available in Azure for automation

**Must have skills : IAM & IGA management**

## Main difficulties / Key Success factors related to the position

Challenges: Come and reinforce the team to reduce the risk of restraint and load

Complexity: Expert in Azure AD in technical deep detail and understand many of back-office architecture. Lots of development required.

## Sizing : Turnover, budget, size of the teams, ...

Infrastructure = +200 Domain Controllers, +200k accounts, +150K mailboxes, +100k devices, +20k mobiles

Teams = 5 experts in France, 6 L3 engineer in India, 1 administrator in Thailand

## Profile

### Educational background

- BE (Bachelor Engineer) minimum
- Experience of at least 10 years on Microsoft identity Technologies
- Experience in international companies with several thousand users
- Experience of AAD integration
- Strong experience in AD management

### Competencies

- Microsoft Identity Manager
- Powershell
- Azure AD
- Azure Automation
- Active Directory
- Anglais
- Windows Server

## Job title

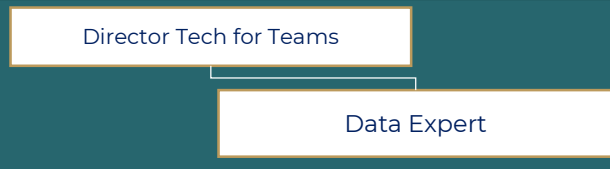
# Data Expert Azure (DataFactory / MS SQL Server Analysis )



## Purpose

Within Tech For Accor Teams, you will participate in implementing and supporting Data-related initiatives for our Corporate Systems applications. Those applications cater to the different headquarters teams of the group as well as the back-office teams of hotels. As a Data Expert, you should also adapt to the range of technologies used by the Delivery team, depending on the specific requirements (Microsoft, SQL, Server / Workloads, Data Cloud, Azure).

## Hierarchical link



## Key interactions

Internally: Property Tech, PMO team , CTS team, Service Delivery team , Digital Factory, VPOs , Hotels

Externally: Management, Owners & Franchise partners, Social partners, Service provider and Suppliers

## Main responsibilities

- Main objectives and responsibilities as a Data Expert:**
- Join the Technical Architecture / Development team
  - Provide expertise in the Data utilization strategy on our Corporate Cloud and OnPremise applications
  - Develop and maintain a data architecture and a data model to ensure data consistency and integrity
  - Perform administration and development of de Pipelines / Datasets / Transformations in Azure Data Factory ETL
  - Conduct Data audits on our OnPrem platforms of Multidimensional Cubes and define data migration strategies
  - Build PowerBI reports using PowerBI Platform

## Technical skills : mandatory for this profile

- Azure Data Factory
- MS SQL Server 2016/2019 ( Analysis Services - Cubes Multidimensional )
- Power BI Platform
- Azure Managed Services (PaaS):
- Azure SQL Database,
- Storage Account

## Technical appreciated skills :

- Azure Data Architecture
- Azure DevOps
- Azure Key Vault
- ARM Templates, Terraform
- Tableau Software

## Soft skills

- Experience : 6 to 9 years
- Proactive, rigorous & committed
- Good synthesis skills and ability to convey information effectively
- Quick learning on projects and ability to work on multiple projects simultaneously.

## Job title

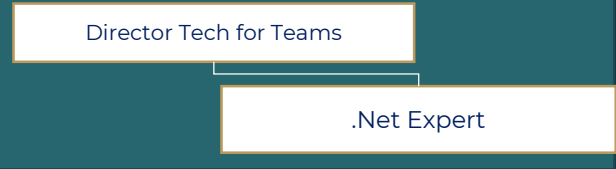
**DotNET Expert**  
(C#/ Web/ MVC/ Azure/AzureDevOps/ MS SQL Server)



## Purpose

Within Tech For Accor Teams, you will participate in implementing and supporting Applications for our Corporate Systems applications. Those applications cater to the different headquarters teams of the group as well as the back-office teams of hotels. As a DotNet Expert, you should also adapt to the range of technologies used by the Delivery team, depending on the specific requirements (Microsoft .Net, SQLServer /Azure Services, Data Cloud, DevOps).

## Hierarchical link



## Key interactions

Internally: Property Tech, PMO team , CTS team, Service Delivery team , Digital Factory, VPOs , Hotels

Externally: Management, Owners & Franchise partners, Social partners, Service provider and Suppliers

## Main responsibilities

## Technical skills : mandatory for this profile

### Main objectives and responsibilities as a DotNet Expert:

- Join the Technical Architecture / Development team
- Act as Tech lead/Expert and provide support for developers and propose technical solution
- Develop and maintain application as fullstack developer
- Perform administration and development of Azure devops Pipelines, Azure app services
- Provide technical support for other teams on Microsoft Technologies
- Act as delivery manager, validate pull requests, assist end users in testing session, manage deployments.
- This profile must have strong .Net/Azure skill to validate all .Net code/solutions developed by the others developers on the team to ensure that the code / solution proposed are correct, optimized cost, maintainable, upgradable and follow security requirement.

- Net framework .NetCore
- MS SQL Server 2016/2019
- Azure platform
- Azure DevOps
- Azure Managed Services (PaaS)
- NodeJS
- Web Development (Angular or ReactJS)

## Technical appreciated skills :

- Azure Data Architecture
- ARM Templates, Terraform
- Tableau Software
- SSAS, SSRS, SSIS
- Legacy frameworks (Nhibernate, NINject, JQuery...)

## Soft skills

- Experience : 10 to 15 years
- Proactive, rigorous & committed
- Good synthesis skills and ability to convey information effectively
- Quick learning on projects and ability to work on multiple projects simultaneously.

5

# *Tech for Hotels*



## Job title

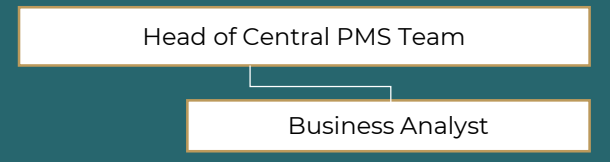
## Business Analyst – Gov Data



## Purpose

To leverage data analytics to drive insights and decision-making within the Hospitality Solutions Team. The Data Analyst will be pivotal in extracting, analyzing, and interpreting data from Oracle Opera Cloud Services and other sources to optimize business processes, enhance guest experiences, and improve operational efficiency.

## Hierarchical link



## Key interactions

### Internally:

Cios in the Region, peers in Property Tech, Tech for Teams, IT Ops, Digital Factory, and IT Infra-structure, network and security.

### Externally:

Third-partner suppliers, Technology architecture forum, peers in the hospitality groups and Data providers and peers in the industry

## Main responsibilities

- Design and implement data collection systems to ensure comprehensive data capture across various operational areas.
- Perform detailed data analysis to identify trends, patterns, and insights that inform strategic decisions.
- Develop and maintain dashboards and reports that provide actionable intelligence to the team and senior management.
- Collaborate with stakeholders to understand data requirements and deliver custom reports and analyses that support specific business objectives.
- Ensure data integrity and compliance with data protection regulations.

## Main difficulties / Key Success factors related to the position

- The role involves managing large datasets from diverse sources and translating complex data into understandable and actionable insights
- Critical issues include ensuring data accuracy, privacy, and security, while adapting to changing business needs and technology landscapes.

## Sizing : Turnover, budget, size of the teams, ...

- Ability to handle extensive datasets with millions of data points across guest experiences, operational efficiency, and financial performance.
- Assisting strategic and operational decisions throughout the organization with critical insights

## Profile

### Typical background & competencies

- Background: Bachelor's degree in Data Science, Statistics, Computer Science, or related field.
- Experience as a Data Analyst, preferably in the hospitality or related industry, with a strong understanding of Oracle Opera Cloud Services.
- Technical Competencies:
  - Advanced proficiency in SQL, Python, or R for data analysis; experience with BI tools (e.g., Tableau, Power BI) for dashboarding and reporting;
  - knowledge of data warehousing and ETL processes.
- Soft Skills: Strong analytical thinking and problem-solving capabilities; excellent communication skills to translate data findings into strategic insights; ability to work collaboratively across teams and with external partners.
- Strong analytical and debugging skills
- Strong communication skills



**Job title**

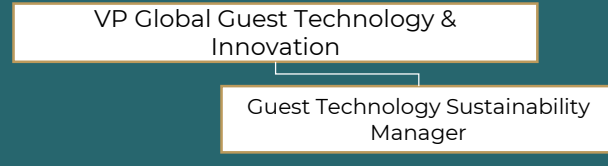
# Guest Technology Sustainability Manager



**Purpose**

In charge of integrating sustainable technology practices and coordinating solutions such as Smart Thermostat, Food Waste Management, Digital directory, Skip the clean, Digital F&B and any other services or product including innovation sustainability opportunity. This role will be responsible for developing and implementing strategies that enhance environmental sustainability through innovative technology solutions.

**Hierarchical link**



**Key interactions**

Internally: Tech 4 hotels teams , Brands Tech leaders, Sustainability team, Operations, DT&S, Procurement, Digital Factory, Loyalty , Security etc

Externally: Suppliers, Sustainability Forums , Focus groups on technology sustainability

## Main responsibilities

**Strategy:** Develop and implement a comprehensive technology sustainability strategy that aligns with the Accor group’s overall environmental goals.

**Drive sustainability projects :** Identify opportunities for reducing the environmental impact of our technology operations, including energy management, waste reduction, and resource optimization.

**Expertise & Enhancements :** Provide technical and functional expertise on sustainable tools used in hotels, prioritize and define with the HUBs. Research and introduce innovative technology solutions that contribute to sustainability, such as renewable energy sources, energy-efficient hardware, and eco-friendly software applications.

**Stakeholder Engagement:** Partnership with Guest Tech procurement on preferred rates and service levels for hotel-based technology, defining new business model, services offers. Collaborate with IT and operational departments to integrate sustainable technologies into everyday practices partnerships and potential innovation programs with key start-up and vendors in the market.

**Industry Trend and Networking:** Responsible to form a sustainability champion community and define the technology standards guidelines to be used and adapted by the hubs. Participate in industry forums and networks to represent the hotel group in sustainability discussions.

**Compliance:** Monitor and report on the effectiveness of sustainability initiatives, providing insights and recommendations for continuous improvement.

## Main difficulties / Key Success factors related to the position

- Finalize Smart Thermostat pilot and deploy it in eligible hotels in PME
- Alignment with sustainability team on Guest Technology sustainable initiatives to provide environmental sustainability through innovative technology solutions.
- Drive Accor tech sustainable projects according to Accor OKRs and KPIs and encourage hotels/ internal team to follow the standards.
- Educate and train staff on sustainable technology practices and their benefits.
- Improve the overall company carbon emissions and produce new innovative ideas to improve the overall result.
- Stay abreast of emerging trends in technology and sustainability, applying best practices to our operations.

## Sizing : Turnover, budget, size of the teams, ...

Nature	Amount
<ul style="list-style-type: none"> <li>• Sustainability Knowledge</li> <li>• Hotels' Operation Knowledge</li> <li>• Hospitality Technology</li> <li>• Project / Build / Implement</li> </ul>	<ul style="list-style-type: none"> <li>• All hotels globally</li> <li>• All brands globally</li> <li>• All sustainable guest-facing technology used in hotels</li> <li>• All projects involving guest technology &amp; innovation</li> </ul>

## Profile

Educational background	Competencies
<ul style="list-style-type: none"> <li>• Bachelor degree in Environmental Science, IT, Sustainability, or related field.</li> <li>• 8years+ experience in a similar role, preferably in the hospitality or technology sector.</li> <li>• Experience in hotel technology, very good knowledge of Accor Central organisation &amp; good relationship with the key vendors in the market</li> </ul>	<ul style="list-style-type: none"> <li>• Strong collaborative and communication skills</li> <li>• Bringing forward proposals / proactive</li> <li>• Curiosity</li> <li>• Resilience</li> <li>• Customer centric &amp; focused on delivering results</li> <li>• Research</li> </ul>

## Job title

# IT Administration & Governance officer



## Purpose

The role of IT Administration and Governance officer is responsible for supporting PMO with general administrative tasks related to Property Tech and Guest Tech Department. This role requires working with cross functional teams and ability to work independently with minimal guidance. Evolution to an executive assistant role.

## Hierarchical link

PMO – Property Tech & Guest Tech – Accor Tech

IT Administrative Officer

## Key interactions

Internally: Service Delivery staff in the Region, All verticals of D&T in the hub, All D&T Operational Teams, SMDL Teams and third-party suppliers team

Externally: Region operations team, Hotel teams, Partner teams, suppliers

## Main responsibilities

- Procurement management: invoicing, purchase orders and other related activities as required
- Budget management: support the budget process: budget initiation, budget templates, actual vs budget analysis
- Governance: support company strategy by following up tasks with PMs and updating reporting, OKR
- Maintain and update project, database and reporting data
- Drafting, editing correspondence, report, and other documents.
- Coordinating travel arrangements and accommodations.
- Handling expenses on the company's expense platform
- Managing email and calendars for team members.
- Scheduling and coordinating appointments and meetings.
- Providing general administrative support as needed.
- Candidate Requirements:
- Strong organizational and time-management skills.
- English fluency (working language)
- Curiosity and ability to learn in a fast pace environment
- Ability to manage recurring tasks, multitask and prioritize tasks effectively.
- Detail-oriented and able to maintain accurate records.
- Ability to work independently and as part of a team.

## Main difficulties / Key Success factors related to the position

- Ability to work independently
- Strong organizational and time-management skills.
- Ability to multitask and prioritize tasks effectively.
- Networking and interpersonal skills

## Sizing : Turnover, budget, size of the teams, ...

- N/A

## Profile

### Educational background

- High school diploma or equivalent; associate's or bachelor's degree preferred.

### Competencies

- 1-3 years of professional experiences
- Excellent communication, pro-active and interpersonal skills.
- Proficiency with Microsoft Office
- Knowledge about procurement and budget process appreciated
- Secretary experience appreciated



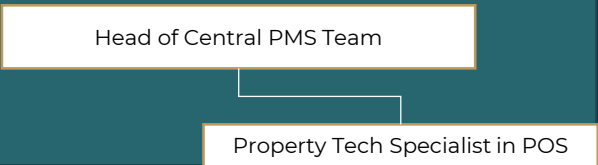
## Job title

# Property Tech Specialist (POS)

## Purpose

The Manager for POS Solutions is responsible for overseeing the operational effectiveness and excellence of the Oracle Hospitality Symphony Point of Sale (POS) system within the organization. This role entails ensuring the POS system aligns with business objectives, enhances customer satisfaction, and optimizes operational efficiency. The manager will lead initiatives for system upgrades, integrations, troubleshooting, and staff training, ensuring the POS ecosystem supports the organization's growth and adaptability to market changes.

## Hierarchical link



## Key interactions

Internally: Work closely with IT, finance, operations, and customer service departments to ensure the POS system meets cross-functional needs.

Externally: Liaise with Oracle Hospitality, third-party integrators, and other technology providers to enhance POS system capabilities and resolve issues.

## Main responsibilities

- System Management and Optimization: Oversee the daily operations of the POS system, ensuring high availability, reliability, and performance that meets the business needs.
- Project Leadership: Lead POS system upgrades, integration with other systems (e.g., Property Management Systems, online ordering platforms), and the rollout of new features or locations.
- Troubleshooting and Support: Act as the primary point of contact for POS system issues, coordinating with IT and vendors for timely resolution.
- Training and Development: Develop and implement training programs for end-users, enhancing staff competencies in utilizing the POS system effectively.
- Data Analysis and Reporting: Utilize POS data analytics to provide insights into sales trends, inventory management, and customer preferences, driving strategic decisions.
- Vendor Management: Manage relationships with Oracle Hospitality and other vendors, ensuring service level agreements (SLAs) are met and negotiating contracts to support business goals.

## Main difficulties / Key Success factors related to the position

- System Integration: Managing the complexity of integrating the POS system with other business-critical systems while ensuring data accuracy and operational continuity.
- Adaptability: Keeping abreast of and adapting to technological advancements and changing business requirements to maintain system relevance and efficiency.
- Security and Compliance: Ensuring the POS system and its integrations comply with industry regulations, data protection laws, and payment card industry (PCI) standards.

## Sizing : Turnover, budget, size of the teams, ...

- Oversee multiple system upgrade projects, integration initiatives, and the expansion of POS capabilities across new locations or business units
- Help manage the POS system budget, including hardware/software procurement, maintenance costs, and vendor contracts.

## Profile

### Educational background & Competencies

- Educational Background: Bachelor's degree in Information Technology or a related field. Certification in Oracle Hospitality Symphony is highly desirable.
- Experience: Minimum of 5 years in a POS system management role, preferably within the hospitality or retail industry. Proven experience in project management, system integration, and staff training.
- Technical Skills: Strong understanding of Oracle Hospitality Symphony
- Soft Skills: Excellent leadership, communication, problem-solving, and negotiation skills. Ability to work under pressure and manage multiple priorities.

## Job title

# Property Tech Manager (Product)



## Purpose

In charge of in staff-facing hotel technology solutions such as Property Management System, Point of sales, Sales & Catering, in hotel payment, SPA and etc. Responsible for implementation and managing relationship with Key vendors / partners ensuring roadmap and implementation is in line with Accor tech Strategy and Accor technology Standards. Responsible to lead projects that will have the involvement of different technology groups, vendors, and operational stakeholders and focus on managing project timelines and budgets, training, communication and adherence to technical and brand standard.

## Hierarchical link



## Key interactions

Internally: Hotel leaders, HUB Operational Teams; HUB IT team, Hub Revenue Management, Global Property Tech team,

Externally: Construction company reps; Technology suppliers and partners; technology support services; peer network, participate on meetings with Assets

## Main responsibilities

- Accountable for project Rollouts, openings and change management to any of the Property Tech solution used on the hotel by the region;
- Accountable and Responsible to define strategy and migration rollout for the change in any property tech solution in the region.
- Working with peers in Accor Tech, business stakeholders and technology providers to develop implementation and training plans.
- Accountable to deliver to the hotels best practices to use the property tech solutions and animate within the Hub trainings, procedures, documentation and communication.
- Provide a strong leadership role and voice on projects to the region, globally and with other internal departments.
- Pro-actively manage implementation scope, changes, issues and outcomes.
- Maintain and promote core property tech standards and maintain best practices in respect to the set up and implementation of property systems.
- Effectively communicate technology related plans, actions and decisions with stakeholders.
- Manage relationships with internal and external stakeholders.
- Contribute to Technology Services knowledgebase.
- Perform other duties as required.
- Accountable for testing and validate the features of the products used within the region;
- Responsible for the guideline and documentation withing the region;
- Give recommendations on the roadmap of functionalities based on the requirement of hotels and fiscal in the region and make decision of prioritization.
- Accountable for looking for hotel productive and new ways of working with automatization and improve process.
- Manage projects from start to finish, including scoping, planning, execution, and post-implementation review.
- Provide guidance and support to team members to ensure the successful implementation of solutions.
- Responsible for interfaces on the troubleshooting, engaging with third-partner suppliers on PMS/POS interfaces & related systems and CRS when applicable.
- Managing functional team for CRS when applicable.

## Main difficulties / Key Success factors related to the position

- Manage schedules between multiple systems and multiple stakeholders & external suppliers;
- Effective manage communication, escalations and conflict of interested with all stakeholders in the region
- A high level of analytical and strategic thinking, as well as exceptional communication skills, is essential to convey complex information effectively.

## Sizing : Turnover, budget, size of the teams, ...

Responsible for Projects and openings budget.  
Responsible for participating on suppliers RFP's and give feedbacks  
Managing a team in property tech  
Overlook for Property Tech system within the Hub scope of Hotels

## Profile

### Educational background & Competencies

- University Degree or equivalent in Computer Science or Hospitality;
- Experience in Managing a team and More than 5 years on a Hospitality Application Role
- Knowledge of key hotel systems: PMS, POS, etc;
- Ability to build strong relationships and maintain a positive reputation.
- Ability to work effectively in high volume, high stress environment
- Understanding of PMS techniques and Cloud strategies.
- Monitor industry trends and best practices to identify new opportunities for process improvement.

## Job title

# Property Tech Specialist



## Purpose

Responsible for implementation of staff-facing hotel technology solutions such as Property Management System, Point of sales, Sales & Catering, in hotel payment, SPA and etc. tech Strategy and Accor technology Standards. Responsible to lead projects that will have the involvement of different technology groups, vendors, and operational stakeholders and focus on managing project timelines and budgets, training, communication and adherence to technical and brand standard.

## Hierarchical link

Property Tech Director

Property Tech Specialist

## Key interactions

Internally: Property Tech, PMO team , CTS team, Service Delivery team , Digital Factory, VPOs , Hotels

Externally: Management, Owners & Franchise partners, Social partners, Service provider and Suppliers

## Main responsibilities

- Responsible for property tech solutions implementation on new openings, rollout and change management
- Provide functional and technical expertise on the property tech solutions and voiced through the governance projects with third-partners and internally
- Organize, drive and/or attend project and related meetings as required.
- Create, Maintain and promote procedures and documentation related to fiscal / legal and local requirements following the Accor standards and maintain best practices in respect to the set up and implementation of property systems.
- Effectively communicate technology related plans, actions and decisions with stakeholders.
- Manage relationships with internal and external stakeholders.
- Provide technical and functional expertise and training hotels and third-partners on Accor knowledge based process.
- Attend hotel operational meetings as required and go to hotels to provide trainings remotely or on site
- Ensure that all legal and country requirements are available and thoroughly considered before implementing any application.
- In charge of communication of hotels for Project, Rollouts and maintenances and change managements.
- Work with cross-functional teams to identify areas for improvement in business operations.
- Develop and propose solutions to improve business processes, increase efficiency, and reduce costs.
- Analyze data and create reports to track progress and measure the success of implemented solutions.
- Responsible for interfaces on the troubleshooting, engaging with third-partner suppliers on PMS/POS interfaces & related systems and CRS when applicable.
- Functional expertise for CRS when applicable.
- Perform other duties as required.

## Main difficulties / Key Success factors related to the position

- Manage schedules between multiple systems and multiple stakeholders & external suppliers;
- Collaborating with IT teams, operational teams, and application providers
- Understanding the specific needs and requirements of hotels to ensure systems are optimized and aligned to hotels needs
- Influence stakeholders' perspectives of requirements and activities.

## Sizing : Turnover, budget, size of the teams, ...

- This role will not be managing people and have no P&L responsibility.
- Strong understanding of priorities and strong understanding of operational process to prioritize requirements to global and suppliers.

## Profile

### Typical background & competencies

- University Degree or equivalent in Computer Science or Hospitality;
- Minimum 2-3 years' experience in the hotel industry in operations or hotel systems.;
- Knowledge of key hotel systems: PMS (Opera Cloud), POS, etc.;
- Ability to build strong relationships and maintain a positive reputation.
- Organized & proactive with the ability to work cohesively as part of a team.
- Good understanding of hotel operations

## Job title

# Revenue Management Success Lead

(18 months contract)



## Purpose

As a member of the Success team, you will play a pivotal role in supporting various projects supporting Accor strategy related to the **deployment of hotel's technologies across the entire portfolio worldwide**, with a particular focus in ensuring consistency in the strategy and deployment process of **Revenue Management Systems (RMS)** and **Property Management Systems (PMS)**

## Hierarchical link

Director of RM Strategy

RM Success Lead

## Key interactions

- Internal: Accor RM & Accor Tech as primary contact. BI, Hubs, Distribution as secondary contact
- External: 3rd party vendors (Both RMS, PMS, and Service providers)

## Main responsibilities

- **Project Management** : Facilitate the onboarding of new hotels with their chosen solution or with a new functionality and support smooth PMS transition in relation to any revenue management solutions. Consistent communication of project status to hotels and internal stakeholders
- **Escalation 'Expertise**: Proactively identify tickets requiring immediate escalation and ensure timely resolution in adherence to our team's service level agreements at Accor. Particular focus in ensuring new onboarded hotels have the necessary technical assistance to set up their software.
- **Second-Level Support**: Serve as the second level of support for Revenue Management Systems and related business processes, addressing questions on System Functionality, Data Configuration, Conceptual/Analytical Questions, Forecast and Decision Questions, Business Processes, Forecast Validation, and Revenue Management Systems Workflows.
- **Team Collaboration – Technology coordinator**: Be the link and facilitator between the Accor Tech team, and the Accor RM team to ensure highest level of coordination and support on any RM topic related technology issue during PMS Changeover or RMS onboarding.
- **Data Analysis**: Conduct ad hoc reports, audits, and analysis as needed, covering topics such as System Usage, Escalated Support Calls, Data Integrity, and System Performance.
- **Third-party Management** : Collaborate very closely with third party vendors on timeline, project plan, and RMS set-up for successful go live/changeover. Providing deep knowledge and experience with RM Solutions including configuration, functionality and troubleshooting in support of:
  - Complex deployment plans.
  - Optimal configuration and usage of the RM solutions.
  - Escalation, arbitration, problem resolution & guidance.
  - Maintain engagement of the user with the tool
  - Maintaining high hotel satisfaction results.

## Main difficulties / Key Success factors related to the position

- **Continuous Learning**: Stay updated on new capabilities launched within Revenue Management systems, and anticipate impact on the entire eco-system
- **Solid Understanding**: Maintain a strong grasp of Accor's Revenue Management business processes, encompassing various brands and current systems, including IDeaS G3, Lite, OTAI, BI tools, S&C Tools, PMS & CRS

## Sizing : Turnover, budget, size of the teams, ...

Excellent verbal and written communication skills.

- Passionate about helping leading hotels to capitalize on revenue management opportunities.

## Profile

### Educational background

- 4+ years hospitality revenue management background, with strong knowledge and understanding of hospitality technology
- Fluent English skills. Second language as a plus (French, Spanish)

### Competencies

- Technology savvy with understanding of BI tools/processes Working knowledge of PMS (property management systems, including Opera Cloud), CRS (central reservation systems), Channel Management, and other hotel systems and onward distribution. Knowledge of Revenue Management Systems, like IDeaS G3 RMS and EzRMS Project management and analytical skills required Self motivated; works well independently with limited supervision Ability to autonomously work in high-pressure situations

6

# *Strategy and Performance*



**Job title**

# Global Projects Communication Manager

01 Dec 2023



**Purpose**

Responsible for defining and deploying the communication plan for major global AT projects plan, aligned on the Accor Tech communications plan. He/She will support all AT Excom members (excluding CTO/Deputy CTO and head of T4H) with communications for their major initiatives and personal thought leadership communications

**Hierarchical link**

Director AT Communications

Global Projects Comms Manager

**Key interactions**

Accor Tech Excom members

Director Accor Tech Communications, Global Communications team

## Main responsibilities

## Main difficulties / Key Success factors related to the position

- Define and deploy the communications plan for all major Accor Tech global projects (excluding Elevate), aligned on the Accor Tech communications plan.
- As communications business partner, support Accor TechExcom members (excluding CTO/Deputy CTO and head of T4H)) with their personal internal and external communication (identifying proactively opportunities and preparing talking points).
- Build key messaging packages for all major Accor Tech projects
- Be ambassador of our #OneTechTeam ambition and mindset and ensure the appropriate change communications and storytelling to accompany the #OneTechTeam ambition for scope of responsibility.
- Contribute actively to the Accor Tech editorial committee and planning for area of responsibility.
- Measure all activity and actions for impact and take data based decisions to ensure continuous improvement.
- Be an active benchmarker, constantly looking outside to learn from others and stay ahead of the curve.

- Be agile and comfortable navigating ambiguity and frequent changes.
- Understanding how to support transformation with adapted change communications
- Being able to understand AT strategy & support and challenge executive leaders
- Capable of partnering with key stakeholders located across geographies & timezones
- Have a global #OneTechTeam mindset
- Ensure inclusive messaging & language so that all AT regions & populations feel recognised

## Sizing : Turnover, budget, size of the teams, ...

- Individual contributor

## Profile

### Educational background

- Minimum 3-5 years experience in a communications business partner role
- Communications cursus and training

### Competencies

- 360° communications skills
- Change Management & Change communications
- AT Business & strategy understanding
- Global mindset & multicultural awareness
- Listening & influencing skills
- Credible & comfortable partnering with senior management
- Excellent storytelling & writing skills
- Excellent English skills both written & oral





RAFFLES \ ORIENT EXPRESS \ BANYAN TREE \ DELANO \ SOFITEL LEGEND \ FAIRMONT \ SLS \ SO \ SOFITEL \ THE HOUSE OF ORIGINALS  
RIXOS \ ONEFINESTAY \ MANTIS \ MGALLERY \ 21C \ ART SERIES \ MONDRIAN \ PULLMAN \ SWISSÔTEL \ ANGSANA  
25HOURS \ HYDE \ MÖVENPICK \ GRAND MERCURE \ PEPPERS \ THE SEBEL \ MANTRA \ NOVOTEL \ MERCURE \ ADAGIO  
MAMA SHELTER \ TRIBE \ BREAKFREE \ IBIS \ IBIS STYLES \ IBIS BUDGET \ JO&JOE \ HOTELF1