UNIBAIL-RODAMCO-WESTFIELD

IT Security Guidelines

Shopping Centre IT Security policies

Table of contents

1 INTRODUCTION 3

1.1 CONTEXT AND SCOPE OF THE DOCUMENT 3
1.2 APPLICABILITY OF THE DOCUMENT 3
1.3 DESCRIPTION OF IT IN THE GROUP'S ASSETS - SHOPPING CENTRE MACROSCOPIC CONFIGURATION 3

2 IT SECURITY ORGANIZATION (ORG) 5

3 DATA PROTECTION (DATA) 6

4 LOGICAL IT SECURITY (LOG) 7

5 IDENTITY & ACCESS MANAGEMENT (IAM) 8

6 NETWORK SECURITY (NET) 9

6.1 TRUST ZONES 9
6.2 INTERNET ACCESS 11
6.2.1 Visitors' Internet access specificities 11
6.2.2 Partners' / Organizer's / Retailers' Internet access specificities 12

7 CRIMINAL SECURITY SYSTEMS (CRI) 13

8 PHYSICAL SECURITY IN IT ZONES (PHYS) 14

9 SYNTHESIS & RACI 15

10 GLOSSARY 19

1 Introduction

1.1 Context and scope of the document

Unibail-Rodamco's Information System hosts an important amount of strategic data which forms the Group's informational heritage which must be protected efficiently. To do so, Unibail-Rodamco has adopted a Global Information Security Policy (GISP) that provides general IT security principles and guidelines to enhance Unibail-Rodamco's Information Security Management.

This document is a translation of the Unibail-Rodamco's Global Information Security Policy (GISP) for the IT implemented within Shopping Centre that are located in different countries. Unibail-Rodamco's Shopping Centres are high-volume transit hubs for thousands of visitors and on different continent in the world. More and more digital services are available to visitors. The protection of the Information Systems available in these zones must be adequate for the different users.

This document defines the requirements regarding IT Security, in order to:

- Limit the risks of the Shopping Centre's Information Systems compromise, which could have a significant and negative impact on the brand image
- Limit the compromise of the Group Information System via the Shopping Centre's Information Systems
- Have a consistent and acceptable IT security level among Unibail-Rodamco's Shopping center assets throughout the Group.

1.2 Applicability of the document

These guidelines must be applied to every IT assets within a Shopping Centre, except IT assets connected to UR corporate network.

There must also be applied to Unibail-Rodamco's providers and partners operating within a Shopping Centre.

The requirements listed in this document, and labelled "**REQUIREMENT**", are mandatory. If a requirement can't be implemented, derogation must be filled and submitted to the IT Security Manager for approval. The derogation requestor must provide all the arguments to justify why the requirement can't be implemented, and propose a corrective action plan.

The recommendations listed in this document, and labelled "**RECOMMENDATION**" are strongly recommended. Best practices are labelled "**BEST PRACTICE**".

1.3 Description of IT in the Group's assets - Shopping Centre macroscopic configuration

A Shopping Centre can be divided in three IT domains:

- Real Estate network : hosts Building Management Systems such as air conditioning or lightning, and safety functions such as video surveillance, intrusion detection and physical access control
- Connected Mall network: hosts the partners' infrastructure and services for visitors. Connected Mall network can also provide Internet connections for retailers.
- Unibail-Rodamco Network: hosts the Shopping Centre management infrastructure.

These three domains are subdivided in trust zones. Each trust zone has specific constraints.

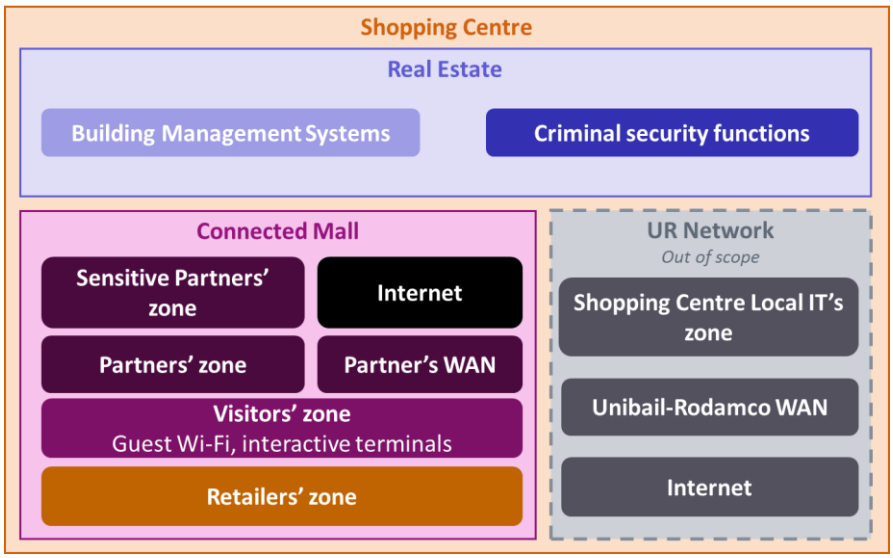

Figure 1 - Shopping Centre trust zones

Note: This document is not applicable to IT assets within UR Network for which other policies and guidelines are applicable.

2 IT Security organization (ORG)

ORG-1	**IT Security Correspondent**	**REQUIREMENT**
The IT Security Correspondent is in charge to check if the requirements and recommendations in this document are applied and is the single point of contact for the IT Security Manager.		

ⓘ The IT Security Correspondent can be local IT manager for regions, or the IT Shopping Centre coordinator for France.

ORG-2	**IT Security Incident**	**REQUIREMENT**
In case of a suspicious event or proven IT security breach, the IT Security Correspondent must be informed within 48 hours. The IT Security Correspondent will then inform the IT Security Manager.		

3 Data Protection (DATA)

Are considered as sensitive data:

- Authentication information
- Personal information (Example Name, address, etc.)
- Credit card information.

Remark: Credit card information is notably used by Gift Cards partners and Parking Management partners.

DATA-1	**Data encryption**	**RECOMMENDATION**
Whenever possible, data should be encrypted in transit and at rest with market standard algorithms.		

DATA-2	**Backups**	**RECOMMENDATION**
Whenever possible and required by business needs, backups should be done and stored remotely.		

DATA-3	**Sensitive data protection regulation and encryption**	**REQUIREMENT**
The processing personal data must be compliant with the European General Data Protection Regulation (“Regulation (EU) 2016/679 of the European Parliament and of the Council”). Those data must be encrypted regarding standards in use on the market		

DATA-4	**PCI-DSS**	**REQUIREMENT**
Partners processing credit card information must have the PCI-DSS certification.		

DATA-5	**Shopping Center data**	**REQUIREMENT**
Any data processed into the Shopping Center can not be in transit into the URW Corporate Network and on the contrary it is mandatory that the shopping centre Network do not handle URW Corporate data		

DATA-6	**IT Outsourcing**	**RECOMMENDATION**
In case of IT outsourcing on data, the Provider commits to maintain an inventory of all IT components processing URW data. Provider also commits to commits to securely destroy data at the end of the service and to provide a destruction statement if it is required by URW.		

4 Logical IT security (LOG)

LOG-1	**Malware protection**	**REQUIREMENT**
When applicable, an antivirus must be installed and kept up-to-date.		

LOG-2	**Patches**	**REQUIREMENT**
IT assets must be kept up-to-date (software, firmware…)		

LOG-3	**Obsolescence**	**REQUIREMENT**
IT assets must be supported from an IT security point of view by the vendor or constructor.		

ⓘ In other words, the vendor/constructor keeps maintaining their product by issuing IT security patches.

LOG-4	**Administration logical interface**	**REQUIREMENT**
Administration logical interface is not accessible from partners' or visitors' network		

LOG-5	**Hardening**	**RECOMMENDATION**
When applicable, IT assets must be hardened with at least the following measures : ▪ Disable unused network ports ▪ Uninstall unused services		

LOG-6	**Remote administration**	**REQUIREMENT**
Remote access to Unibail-Rodamco's IT assets must be done by using a jump-off server hosted in a DMZ.		

LOG-7	**Retention period of IT assets events**	**RECOMMENDATION**
The following event should be recorded regarding Local regulations: - Used logging: timestamp, user ID and terminal ID, success or failure of the attempt - Actions needing high privileges: timestamp, user ID, action description, success or failure of the attempt - Actions by authorized users on security settings: timestamp, user ID, type of action, object name on which the action is done		

5 Identity & Access Management (IAM)

The Identity and Access Management policy must be applied. The following requirements are additional measures to the ones available in the Identity and Access Management policy.

IAM-1	**Default accounts**	**REQUIREMENT**
Whenever technically possible, default and guests accounts must be deleted or disabled.		

IAM-2	**Default account's passwords**	**REQUIREMENT**
If not disabled, default accounts' password must be modified with a password that complies with Unibail-Rodamco's password policy.		

IAM-3	**Use of nominative accounts**	**REQUIREMENT**
Whenever possible, each stake holder interacting with Unibail-Rodamco's IT assets must be identified with a nominative account and their authorizations must be clearly defined.		

IAM-4	**Shared account management**	**REQUIREMENT**
In the event shared accounts are necessary, the login and password must be stored securely.		

ⓘ *This kind of information can be stored in a password vault for instance*

IAM-5	**Least privileged principle**	**REQUIREMENT**
Users' authorizations must be granted following the least privilege principle. Users must not have high privileges (administrator) on their workstations.		

IAM-6	**Multi-factor authentication**	**BEST PRACTICE**
Access to sensitive function should be done with multi-factor authentication.		

IAM-7	**Authorization matrix**	**BEST PRACTICE**
Each user's authorizations to a Unibail-Rodamco's sensitive IT asset (safety functions, sensitive servers…) should be logged, continuously updated and yearly reviewed.		

6 Network Security (NET)

6.1 Trust zones

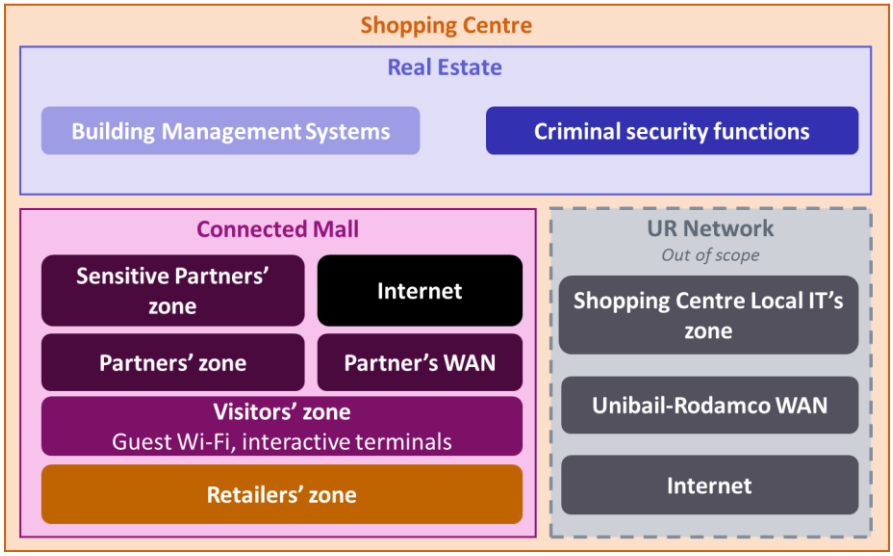

Figure 2 Shopping Centre's trust zone

NET-1	Partners' trust zone	REQUIREMENT
Each partner (whether sensitive or not) corresponds to a single and dedicated trust zone.		

NET-2	Safety functions' trust zone	REQUIREMENT
Each safety function corresponds to a single and dedicated trust zone.		

ⓘ *Some safety functions are submitted to local regulation, as for instance regarding fire protection functions*

NET-3	Trust zones' borders	REQUIREMENT
Each inbound and outbound communication to and from trust zones must be filtered.		

NET-4	Filtering policy	REQUIREMENT
Filtering functions must implement the following principle : "Everything that has been not explicitly approved must be forbidden"		

ⓘ *In other words, the firewalls must only authorize data flows that have been explicitly defined (white list principle).*

NET-5	**Communications between trust zones**	**REQUIREMENT**
Communications between the Shopping Centre and Exhibition venue's trust zones must be limited to the strictly minimum and necessary justified.		

ⓘ By default, the communication between trust zones must comply with the following network flow matrix:

- *Cells in **red** : Not allowed*
- *Cells in **orange** : Allowed under specific conditions*
- *Cells in **green** : Allowed*
- *Cells in **grey** : Not applicable*

Source : ↗ Destination :		**Real Estate networks**			**Connected Mall networks / Digital services network**							**UR Network**	**Internet**
		BMS	Criminal security	Criminal security systems Y	Sensitive partner 1	Sensitive Partner 2	Partner A	Partner B	Partner A's network	Partner B's network	Visitors	Organizers (Viparis)		
Real Estate networks	BMS													
	Criminal security systems X													
	Criminal security systems Y													
Connected Mall networks / Digital services network	Sensitive partner 1													
	Sensitive partner 2													
	Partner A													
	Partner B													
	Partner A's network (via its WAN or VPN)													
	Partner B's network (via its WAN or VPN)													
	Visitors													
	Organizers (Viparis)													
UR Network														
Internet														

Figure 3 - Network flow matrix

6.2 Internet Access

Shopping Centre provides:

- A Wireless Internet connection to its visitors
- A Wired and/or Wireless Internet connection to partners / organizes

NET-6	**Internet Access Logs**	**REQUIREMENT**

Internet traffic must be logged according to the local law and regulations constraints.
Logs must contain at least the following information :

- MAC address of the device
- Timestamp
- Target URL and/or IP address

As for example, filtering can be done:

- *With a captive portal for visitors*
- *With a firewall for partners / organizers*

6.2.1 Visitors' Internet access specificities

NET-7	**Visitors Internet Access**	**REQUIREMENT**

In order to be compliant with local laws and regulations, visitors must approve the Use Conditions prior to using the Internet Access provided by the Shopping Centre / Exhibition venue.

NET-8	**Visitors - Web filtering**	**REQUIREMENT**

Visitors' Internet traffic must be filtered in order to prevent the access to illegal and inappropriate contents.
The categories to be blocked are the following (not exhaustive) :

- Illegal content
- Adult content
- Aggressive content
- Drugs
- Weaponry
- Copyright-infringement websites

NET-9	**Visitors' WIFI – Configuration**	**REQUIREMENT**

Visitors' WIFI infrastructure must be configured securely by implementing at least the following measures :

- Protection against ARP poisoning
- Protection against DNS Hijacking
- Protection against intrusions
- Protection against Rogue AP

ⓘ The following measures can be implemented (depending on the vendor and architecture in place):

- *DHCP Snooping*
- *Network isolation (VLANs) and filtering (via firewall or ACLs)*
- *No administration interface available from the Visitors' WIFI*

NET-10	**Visitors' WIFI – Device isolation**	**REQUIREMENT**

Visitors' devices must not be able to communicate with each other through the Visitors' Wi-Fi.

NET-11	**Visitors' WIFI – Exposure to the Internet**	**REQUIREMENT**

Only the necessary ports for a standard usage of the Internet must be opened from the Wi-Fi network to the Internet:

- Web protocols (HTTPS)
- Email synchronization (IMAP)
- Protocols required by the Shopping Centre / Exhibition venues' mobile app

6.2.2 Partners' / Organizer's / Retailers' Internet access specificities

NET-12	**Partners / Organizers / Retailers - Web filtering**	**RECOMMENDATION**

Partners' Internet traffic must be filtered in order to prevent the access to illegal and inappropriate contents.
The categories to be blocked are the following (not exhaustive) :

- Illegal content
- Adult content
- Aggressive content
- Drugs
- Weaponry
- Copyright-infringement websites

7 Criminal Security Systems (CRI)

CRI-1 Network	**REQUIREMENT**
The criminal security systems' network must be a wired network	

CRI-2 Network isolation	**REQUIREMENT**
The criminal security systems must be logically isolated and must not communicate with other networks	

CRI-3 Physical network isolation	**RECOMMENDATION**
When applicable, the network infrastructure hosting the criminal security systems (for instance cables, switches, routers) should be physically isolated from the other networks.	

CRI-4 Internal / External isolation	**RECOMMENDATION**
When possible, networks hosting the external and internal criminal security systems (cameras, monitoring stations, badge reader, detectors…) should be isolated.	

CRI-5 Administration interface	**REQUIREMENT**
The administration interfaces must only be accessible from the criminal security systems' network.	

CRI-6 Device isolation	**RECOMMENDATION**
Accessible criminal security IT assets (cameras, detector, badge reader…) must not be able to communicate with each other.	

ⓘ This could be implemented by hosting all the cameras in an Isolated PVLAN and filter the communications from the routing equipment (via ACLs or via firewall rules).

CRI-7 Criminal security systems data flow	**RECOMMENDATION**
When applicable, criminal security systems' data (video, administration) flow should be encrypted and authenticated.	

ⓘ The protocol used must protect against replay attacks, such as TLS or IPsec.

8 Physical Security in IT Zones (PHYS)

An IT zone is a location in which IT components are hosted. It can be either Offices, IT rooms or network bays.

PHYS-1	**Non-public IT zones**	**REQUIREMENT**

Non-public IT zones must be protected against physical intrusion :

- Access control:
  - Badges for IT rooms or offices
  - Keys or code for network bays that are not hosted in IT rooms
- Anti-intrusion alarms
- Video surveillance with detector on the zone hosting IT components

ⓘ The use of codes to protect IT rooms is tolerated until a badge system is installed. In such cases, access codes must be renewed on a yearly basis.

PHYS-2	**Access codes**	**REQUIREMENT**

Access codes must be renewed every year.

PHYS-3	**Protection of accessible ports**	**REQUIREMENT**

Every access (network ports, network cables, switches, Wi-Fi routers, USB ports…) that might be accessed by anyone in public zones and that is connected to Unibail-Rodamco's Information System must be hidden and/or disabled.

PHYS-4	**Technical room access log**	**REQUIREMENT**

Access to technical rooms must be logged.

PHYS-5	**Partners accesses to IT technical rooms**	**REQUIREMENT**

If a partner requires an access to the technical rooms, it must be escorted by an authorized person and its visit must be logged in a visitors' register.

9 Synthesis & RACI

Responsible **A**ccountable **C**onsulted **I**nformed		**Corporate Teams**	**Asset**	**IT provider (outsourcer)**	**Partner**	**Other**
IT Security Organization						
ORG-1 IT Security Correspondent	**REQ.**	AR				
ORG-2 IT Security Incident	**REQ.**	A	R	R	R	R (anyone)
ORG-3 Audits	**REQ.**	AR				
Data Protection						
DATA-1 Sensitive data encryption	**REQ**		A	R (authentication data)	R (authentication data + credit card data)	
DATA-2 Data encryption	**REC.**	I		AR (Connected Mall provider on their scope)	AR (on their scope)	
DATA-3 Backups	**REC.**	I		AR (Connected Mall partner - on their scope)	AR (on their scope)	AR (on their scope)

Responsible **A**ccountable **C**onsulted **I**nformed		**Corporate Teams**	**Asset**	**IT provider (outsourcer)**	**Partner**	**Other**
Logical IT Security						
LOG-1 Malware protection	**REQ.**			AR (on their scope)	AR (on their scope)	
LOG-2 Patches	**REQ.**			AR (on their scope)	AR (on their scope)	
LOG-3 Obsolescence	**REQ.**			AR (on their scope)	AR (on their scope)	
LOG-4 Administration logical interface	**REQ.**			AR (on their scope)	AR (on their scope)	
LOG-5 Hardening	**REC.**			AR (on their scope)	AR (on their scope)	
LOG-6 Remote administration	**REQ.**	A (IT)		R (Connected Mall partner)	R	
Identity & Access Management						
IAM-1 Default accounts	**REQ.**			AR (on their scope)	AR (on their scope)	
IAM-2 Default account's passwords	**REQ.**			AR (on their scope)	AR (on their scope)	
IAM-3 Use of nominative accounts	**REQ.**			AR (on their scope)	AR (on their scope)	
IAM-4 Shared account management	**REQ.**			AR (on their scope)	AR (on their scope)	
IAM-5 Least privileged principle	**REQ.**			AR (on their scope)	AR (on their scope)	
IAM-6 Multi-factor authentication	**B.P.**			AR (on their scope)	AR (on their scope)	
IAM-7 Authorization matrix	**B.P.**			AR (on their scope)	AR (on their scope)	

Responsible **A**ccountable **C**onsulted **I**nformed		**Corporate Teams**	**Asset**	**IT provider (outsourcer)**	**Partner**	**Other**
Network Security						
NET-1 Partners' trust zone	**REQ.**	A (IT)		R (Connected Mall partner)		
NET-2 Safety functions' trust zone	**REQ.**	A (IT)		R (Connected Mall partner)		
NET-3 Trust zones' borders	**REQ.**	A (IT)		R (Connected Mall partner)		
NET-4 Filtering policy	**REQ.**	A (IT)		R (Connected Mall partner)	C	
NET-5 Communications between trust zones	**REQ.**	A (IT)		R (Connected Mall partner)	C	
NET-6 Internet Access Logs	**REQ.**	A (IT)		R (Connected Mall partner)		R (captive portal)
NET-7 Visitors Internet Access	**REQ.**	A (IT)		R (Connected Mall partner)		R (captive portal)
NET-8 Visitors - Web filtering	**REQ.**	A (IT)				R (captive portal)
NET-9 Visitors' WIFI – Configuration	**REQ.**	A (IT)		R (Connected Mall partner)		
NET-10 Visitors' WIFI – Device isolation	**REQ.**	A (IT)		R (Connected Mall partner)		R (captive portal)
NET-11 Visitors' WIFI – Exposure to the Internet	**REQ.**	A		R (Connected Mall partner)		R (captive portal)
NET-12 Partners / Organizers / Retailers - Web filtering	**REQ.**	A (IT)		R (Connected Mall partner)		

Responsible **A**ccountable **C**onsulted **I**nformed		**Corporate Teams**	**Asset**	**IT provider (outsourcer)**	**Partner**	**Other**
Criminal Security Systems' Security						
CRI-1 Network	**REQ.**	A (PMPS)	R	R (real estate provider)		
CRI-2 Network isolation	**REQ.**	A (PMPS)	R	R (real estate provider)		
CRI-3 Physical network isolation	**REC.**	A (PMPS)	R	R (real estate provider)		
CRI-4 Internal / External isolation	**REC.**	A (PMPS)	R	R (real estate provider)		
CRI-5 Administration interface	**REQ.**	A (PMPS)	R	R (real estate provider)		
CRI-6 Device isolation	**REC.**	A (PMPS)	R	R (real estate provider)		
CRI-7 Criminal security systems' data flow	**REC.**	A (PMPS)	R	R (real estate provider)		
Physical Security in IT zones						
PHYS-1 Non-public IT zones	**REQ.**		AR			
PHYS-2 Access codes	**REQ.**		AR			
PHYS-3 Protection of accessible ports	**REQ.**		AR			
PHYS-4 Technical room	**REQ.**		AR	R (real estate provider)		
PHYS-5 Technical room access log	**B.P.**		AR	R (real estate provider)		
PHYS-6 Partners accesses to technical rooms	**REQ.**		AR			

10 Glossary

GISP	Global Information Security Policy. Founding document of the security documentation base. It describes the terms of reference of the information security: global security principles, organisation and responsibilities.
Information security incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information system	Applications, services, information technology IT assets, or other information handling components.
OISP	Operational Information Security Policy. Extension of the GISP in founding security rules, in compliance with the ISO 27002:2013 standard. The OISP defines the security requirements to be applied to contribute to the information system security.
Risk	Potential that threat will exploit vulnerabilities of an information IT asset or group of information IT assets and thereby cause harm to the organisation. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.
Security requirement	Need or expectation that is stated (documented information), generally implied (common practice) and obligatory.
User	Every internal or external individual who might access to the UR information system.
Default account	Accounts that are being installed by the vendor or constructor into their products. Usually these accounts have important privileges. Default accounts and their password are commonly widely known by the hacker community (and also available on the Internet).
Criminal security system	Criminal security systems are integrated systems or business functions aimed to protect assets from criminal events. These systems can gather video surveillance, anti-intrusion and physical access sub-systems.
Cybersecurity / IT security	Cybersecurity is the generic term for the logical security of IT components (IT hardware, firmware, software…).
Safety system	Safety system are aimed to protect assets from natural events (example: fire)
IT zones	Zone hosting IT components. Can be either offices, IT rooms or network bays.