riscogroup.com



RISCO Cloud Remote Management Solution





Web User Application

User Guide

For more information about RISCO Group's branches, distributors and full product line, please visit **riscogroup.com**

Contents

Introduction	3
Self Registration	4
Login	8
The Home Page	11
Main Screen	11
Cameras Panel	12
Status Panel	12
Security Screen	13
Partitions	13
Arming and Disarming	14
Arm and Disarm the System	14
Cameras Screen	15
Filter Cameras Screen	15
Edit Camera Name	17
Capture and Download Image	17
Save Video Clip	17
Detectors Screen	18
Filter Detector Screen	18
Edit Detector Name	18
Bypass and Un-bypass Detectors	19
Automation Screen	20
Activate and Deactivate Utilities	20
Event History Screen	21
Filter Event History Screen	21
Download and Print the Event Log	22
View Alarm Event Snapshot Images	22
Users Screen	23
Users and Permission Settings	24
Adding a New User and New CP User	24
Follower Settings	30
System Settings Screen	32
Editing Site Details	33
Date and Time Settings	34
Standard Limited Product Warranty	35
Contacting your Installer / Supplier-Agent	37
Contacting RISCO Group	37

Introduction

The RISCO Cloud Remote Management Solution is made up of an alarm panel, various detectors, IP network cameras, a Smart Home system, video equipment and a number of optional peripheral devices.

The **Control System** is the brain of the system. It communicates with all the devices connected to the system. For example, in the event of a burglary, a detector sends a signal to the control system indicating that it has sensed motion on the premises. On receiving this signal, the control system makes the decision to report the alarm to your monitoring service and activate the siren.



Detectors & Accessories are the devices that protect your home, alerting the control system when there is a breach in security. Magnetic contacts protect your doors and windows while motion detectors in combination with IP cameras are able to detect and display an intruder moving across its field of view.



Keyfobs are hand-held transmitters that are used to operate the system. Various keyfobs are available providing a number of functions. For example, arming and disarming the system and sending panic alarms.

Keypads enable you to communicate with the control system in order to perform a number of different functions. The main function you can perform using a keypad is to arm the system when leaving your home and to disarm on your return.

The control system includes a built-in internal siren that is sounded during certain alarm conditions to warn you and deter intruders. When an event occurs during system monitoring, the control system sends a message to your monitoring service via the **RISCO Cloud** describing the exact nature of the event. This enables the monitoring service to take the required action.



The **Web User Application** provides a full interface to your system from a local or remote PC. Via the **RISCO Cloud** you can perform a wide range of tasks, such as, arm/disarm, video snapshot and live streaming, detector bypass, user code management and home utility automation control.



The **Smartphone Application (iRISCO)** provides access to the **Web User Application** from your Smartphone (iPhone or Android).

Self Registration

The Web User Application requires the end user to register in order to gain access to a Site.

A Site represents a physical location in the RISCO Cloud where equipment is installed and through which the Installer can manage a control panel, IP Cameras and a Smart Home system

To Register to the RISCO Cloud:

1. Enter the Web page address supplied by your service provider into your browser and press <Enter>. The Login page displays.

Creating Security Solutions.
Username/Email Address
Password
Remember me
Log In Register Lost password?
© 2019 All rights reserved to RISCO Group LTD www.riscogroup.com

Figure 1 Login Page

NOTE: If you have already registered but forgotten your Login details, click the Lost Password link to request the password to be sent to your email address.

- 2. At the top right of the screen, select English from the language list.
- 3. Click the Register link. The Self Registration page displays.

G Crea	ating Security Solutions.
Email Address	Your Email address will be used as your login name
Full Name	
Create Password	LAt least 8 chars. small and upper case
Retype Password	L Retype password show
Site Name	
Country	United Kingdom of Great Britain and Northern Ireland 🚽
County / Province	
Time Zone	(GMT+00:00) Greenwich Mean Time : Dublin, Edinburgh 👻
City	
Address	
Post Code	
Phone	
Equipment Type	Control Panel
Equipment Id	SN for panel or MAC for other equipment
System PIN	
HGWG Re-Generate	Enter the symbols you see on the image



Figure 2 Self Registration Page

4. Enter the following registration details into the Self Registration page.

Field	Description
Email Address	Enter your chosen Login Name (i.e. email address) NOTE: Only one email can be used for multiple sites.
Full Name	Enter your First and Last Name
Create Password	Enter your chosen Password. The password must be a minimum of eight characters and must contain at least one capital letter, one small letter and one special symbol
Retype Password	Enter again your password
Site Name	Enter a suitable name for your Site
Country	Select your country

Field	Description
County / Province	Select your county or province, if applicable
Time Zone	Select your location time zone
City, Address, Post Code and Phone	Enter these details
Equipment Type	Select the equipment type: control panel, IP Camera, Smart Home Gateway and NVR
Equipment ID	Enter the control panel's Serial Number. For other equipment enter the MAC address
System PIN	If the selected equipment is a control panel, enter its PIN Code
Captcha Code	Enter the Captcha code exactly as its displayed
Terms and Conditions Agreement	Read the Terms and Conditions Agreement and check the checkbox to continue

NOTES:

- a. The Login details entered must not be shared with other users.
- b. All the fields are mandatory.
- c. Select one of the options for staying in touch.
- d. Make sure to select the Terms & Conditions box before you complete the registration.
- 5. Click Register. The Self Registration process sends a confirmation email to your specified email address.
- From the received email, click the attached link to confirm your registration. The Login page is displayed and you can now login to the Web User Application.

Login

To enter the Web Application from within your browser, enter the Web page address supplied by your service provider and press <Enter>. The Login page is displayed.



Figure 3 Login Page

To login to the Web User Application:

1. Enter your User Name (email) and Password that you defined during the registration process.

NOTE: Select the "Remember me" box for the system to remember your login details for next login.

2. Click Login.

NOTE: You can change your password on the Login page by clicking on "Lost Password".

Creating Security Solutions.
Sites Available For You: Brown Residence Matter/Owner Commpact Site Matter/Owner
Site PIN Code Login I am not user 'John@gmail.com' Create a new site Retrieve Sites

Figure 4: Site Selection

- 3. Select one of the displayed sites. Figure 4 shows an example of a user registered to two sites.
- 4. Enter the Site PIN Code.
- 5. Click Login.

NOTE: Clicking "I am not user `x@x.xxx" will take you back to the Login page.

If you want to create a new site as an existing user, click the "Create a new site" link. Then, enter the relevant details as when registering to the RISCO cloud (as described above).

R G Crea	ting Security Solutions.
Site Name	L]
Country	United Kingdom of Great Britain and Northern Ireland
County / Province	
Time Zone	(GMT+02:00) Jerusalem
City	
Address	
Post Code	
Phone	
Equipment Type	Control Panel
Equipment Id	SN for panel or MAC for other equipment
System PIN	
	Create
acree to terms and conditions	Back To Sites' List
- agree to <u>terms and contactoris</u>	
© 2019 All rights r	eserved to RISCO Group LTD www.riscogroup.com

Figure 5: Creating a New Site

NOTE: Since you are an existing user in the cloud, only the site details are required as your personal details are already registered.

The Home Page

After login, your system's home page is displayed (see below). The section following describes the main elements of the System Overview.



Figure 6: System Overview

Main Screen

The Main Screen offers the menus (user links) to various pages in the Web Application as well as the Log Off button. The following menus are available from the Main Screen.

Menu	Description	
Overview	Selecting Overview allows the user to return to the Main Screen at any time.	
Security	Used for arming and disarming the system.	
Cameras	Used for viewing the system cameras (can be filtered by all cameras, live video cameras or still cameras).	
Detectors	Used for viewing detectors (can be filtered by all, triggered or bypassed).	
Automation	Used for the automation and scheduling of appliances.	

Menu	Description
Event History	Used for the viewing of a history log of events (can be filtered by alarms, errors and date).
A Users	Used to define system users.
System Settings	Used for defining system date / time settings.
ے Logout	Used to logout from the Web User Application

Click the Close / Open button to toggle between closing and opening the Main Screen.

Cameras Panel

The Cameras panel opens in "multiple camera view". This view displays snapshots of all the IP and PIR cameras currently being monitored in the system.



Figure 7: Cameras Panel

This view refreshes automatically every 10 seconds.

Clicking on one of the camera frames opens the "single camera view".

Status Panel

The Status panel displays information on your system's status. This status information is displayed according to the local time at the control system.

Last Arams	Bypassed Detoctors	System Status	
11/8 12:30 IT Rooms Activation	11/8 12:30 Entrance Front Door	Armed: 11 Partitions	
11/8 05:40 Main Corridor 😤	11/8 05:40 End Corridor	Disarmed: 2 Partitions	
9/8 07:32 Main Entrance	9/8 07:32 Partking 12	Partially Armed: 1 Partitions	

Figure 8: Status Panel

This view displays the last alarms that entered the system, the detectors that were last bypassed and the overall arm / disarm status of the partitions within the system. Clicking on any of the windows opens the event log/ detectors / security tabs correspondingly.

This view refreshes automatically.

Security Screen

Ô

Selecting the Security Menu displays the Security Screen (see below). This screen is used for arming and disarming the system.

RISCO GRECOUNTORS Creating Security Solutions.	SECURITY [®]			
Overview	Partitions	PARTIAL	DISARMED	ARMED
oo ⊡t Cameras	Lobby			
Detectors	Offices			
G Automation	Server Room			
Event History	Warehouse			
{ွ်} System Settings				
දා Logout				
← Close				

Figure 9: Security Screen

You can also view the current arm/disarm status of the entire system or individual partitions.

Partitions

Monitored areas can be divided into partitions. You can think of each partition as a separate security system that can be armed and disarmed individually regardless of the condition of any other. Partitions can be armed or disarmed one at a time or all at once, and each partition can be assigned as fully armed or part armed. Please refer to the relevant control system installation manual for the number of partitions that can be defined.

NOTE: Partitions are only available in the Web User Application if they have been pre-defined in the control system.

Arming and Disarming

Arming can be defined as turning the system on. When the system is armed, it monitors the areas that are protected by the detectors. If a detector detects an intrusion, the system generates an alarm. Certain detectors can be programmed to be active 24 hours a day (e.g. Flood, Gas and Panic zones). These detectors are always active regardless of system status.

The following arming / disarming options are available from the Security Screen:

Option	Description
Partial	Part arming enables you to arm certain areas of your premises while at the same time remaining in a different part of the premises
Disarmed	Disarming deactivates the entire system. This method is used when you intend to stay, utilizing all areas of the premises
Armed	Full Arming activates the entire system. This method is used when you intend to go out, leaving your premises empty

NOTE: Before arming the system, check that all doors and windows (zones) are closed. This ensures that the system is ready for arming. If a zone is open when trying to arm the system, a popup message displays.



Figure 10: System Not Ready Message

NOTE: Either click the Bypass Detector and Arm button or select the Do not arm option.

Arm and Disarm the System

On the Security Screen, click the Armed or Partial options (see Arming and Disarming).

Disarming, by clicking the Disarmed option, can be regarded as turning the security system off. A user code is required in order to disarm the system.

Cameras Screen

00

Selecting the Cameras Menu displays the Cameras Screen (see below). This screen is used for viewing the system cameras (can be filtered by all cameras, live video or still cameras). You can also customize the camera view, edit the name of the camera, take a snapshot and download the captured image.



Figure 11: Cameras Screen

Filter Cameras Screen

Select the relevant camera view filtering option.



The Camera Screen can be filtered by: All Cameras, Live Video (Indoor / Outdoor IP Cameras) or Still Cameras (PIR Cam).

You can also use the following camera view options:



Figure 12: Multiple Camera Screen (Snapshots only)

With the Multiple Camera Screen **bib** displayed you can view snapshots from all installed cameras. This view refreshes every 15 seconds.

Click the Mand icons to expand and compress the partition camera views.





Figure 13: 2x2 Camera Screen (Snapshots only)



Figure 14: 3x3 Camera Screen (Snapshots only)

With the 2x2 / 3x3 Camera Screen displayed, click the ticon to add a camera to the selected frame.



Figure 15: Single Camera Screen (Live Video and Snapshots)

Edit Camera Name

With the Single Camera Screen displayed, select the required camera and click the comera name field accordingly.

Capture and Download Image

With the Single Camera Screen displayed, click the Take Image button to capture the currently displayed image. Download the captured image by clicking the adjacent Download Image button. The image will be saved on the computer's local drive.

Save Video Clip

With the Single Camera Screen **b** displayed, right-click on the video clip and select "Save video as". Browse to the desired folder and click Save.

Detectors Screen

Selecting the Detectors Menu displays the Detectors Screen (see below). This screen is used for viewing detectors (can be filtered by all, triggered or bypassed). You can also edit the name of a detector as well as bypass and unbypass detectors.

RISCOP creating Security Solutions.	DETECTORS			
Overview	ALL TRIGGERED	BYPASSED		
Security	🗸 Lobby 🛅			
oO ☐₁ Cameras	🛓 Demo Zone	Entrance	Uindow	
Detectors	✓ Offices			
🖒 Automation	Window	Gffice1	Gffice2	Gffice3
Event History	🗸 Server Room 🕞			
A Users	Window	🖹 Server Room		
၄ ်္ဘဲ System Settings				
← Close	Window	Ceiling		

Figure 16: Detectors Screen

Filter Detector Screen

Select the relevant detectors view filtering option tab.

ALL TRIGGERED BYPASSED

The Detectors Screen can be filtered by All (detectors), Triggered (detectors) or Bypassed (detectors).

Click the \mathbf{V} and \mathbf{N} icons to expand and compress the area views.

Edit Detector Name

Select the required detector. When the detector popup displays, click the icon and edit the detector name field accordingly.

Bypass and Un-bypass Detectors

A bypassed detector is ignored by the system and does not generate an alarm when triggered. To "un-bypass" a detector is to restore the detector, effectively instructing the system to continue monitoring activity from that detector.

Select the required detector. When the detector popup is displayed, click the Bypass / Un-bypass Detector option.

NOTE: All bypassed detectors are automatically set to un-bypass when the system is disarmed.

Automation Screen

Selecting the Automation Menu displays the Automation Screen (see below). This screen is used for the control of home-based utilities (appliances, lights, etc.).



Figure 17: Automation Screen

Activate and Deactivate Utilities

Click the relevant utility switch **Solution** to toggle between Turn On (activate) and Turn Off (deactivate), or, by Trigger (provides a pulse as an output).

Event History Screen

Selecting the Event History Menu displays the Event History Screen (see below). This screen is used for the viewing a history log of events (can be filtered by alarms, errors, all or custom). For each event you can view the date and time that the event occurred, a description of the event and the detector or device that caused the event.

RISCOP creating Security Solutions.	EVENT HISTORY	
८ ℃ Overview	ALARMS 🛕 ERRORS ALL CUSTOM 🛱 🕁 🔍	10
Security	✓ October 1-16 (2)	
oO Cameras	09 10:30 AM Alarm - 'Lobby', 'Demo Zone' 跲	
Detectors	07 3:59 PM Alarm - 'Lobby', 'Demo Zone' 🛱	
Automation	✓ July (3)	
Event History	17 3:36 PM Alarm - 'Lobby', 'Demo Zone'	
8 Users	17 3:02 PM Alarm - 'Lobby', 'Demo Zone' 17 2:58 PM Alarm - 'Lobby', 'Demo Zone'	
င်္ဂြို System Settings		
ے Logout	> June (19)	
← Close	> May (19)	

Figure 18: Event History Menu

You can download and save the log to a pre-formatted file type or simply print the log. You can also view captured snapshot images recorded during specific camera related alarm events. These events are indicated with the \square icon.

Filter Event History Screen

Select the relevant event history view filtering option tab. The Event History Screen can be filtered by Alarms, Errors or All. You can also use the following event search options:

Option	Description
Q	Search for specific events (the results of the search appear under Custom)
t 12	Search for events according to specific dates

Download and Print the Event Log

You can download (in .xls format) and save the log to a pre-formatted file or simply print the log. You can also use the following download and print options:

Option	Description
~)	Download and save the event history log
G	Print the event history log

View Alarm Event Snapshot Images

Select the required alarm event and click the 🛱 icon. The selected alarm event snapshot image is displayed.



Figure 19: Alarm Event Snapshot

Users Screen

8

Selecting the Users Menu displays the Users Screen (see below). This screen is used for defining system users, user authority levels / permissions and follower notification settings.

RISCOP Creating Security Solutions.	USERS		
👌 Overview	USERS & PERMISSIONS	FOLLOWERS	
Security	< John Brown		
Detectors	Personal Details:	John Brown	•
Automation	Name *		•0
Event History	Email Address	-445547321 &	\square
A Users	Country *	United Kingdom of Great Britain a	Add Photo
ို္ပ်ို System Settings	County / Province		
🖒 Logout	City *	London	
← Close	Address *	56 Croster Street	
	Post Code *	123435	
	Security System Acces	ss: 🗸	
	User Code *		Check
	Sh	now Code	
	Authority Level	Jser 👻	
	Partitions *	Choose partitions *	
	Language	English (UK) 👻	
	Notifications Add		
	Save	Close	

Figure 20: Users Screen

Users and Permission Settings

The Users and Permissions tab is used for defining the system user's details and managing the authority levels and permissions of each system user.

The Grand Master authority level is used by the system owner and is the highest Authority Level. The Grand Master has full permissions. In addition, only the Grand Master can add a New User and set their permissions.

For other user authority levels/permissions, see below.

Adding a New User and New CP User

You can add a New User and a New CP User to the system. A user has an account in the cloud and can operate the security system remotely from the cloud or locally from a keypad. A CP user can operate the security system locally from a keypad.



RISCOP creating Security Solutions Marcane	USERS
🔗 Overview	USERS & PERMISSIONS FOLLOWERS
Security	+ Add New User + Add New CP User
Detectors	Y30 (Grand Master)
Automation	C. 8087 varone30@riscogroup.com
Event History	
A Users	User1 (User)
දිටු System Settings	
🖒 Logout	
$\leftarrow Close$	



1. Click Add New User to open the New User settings

Creating Security Solutions	USERS
Overview	USERS & PERMISSIONS FOLLOWERS
Security	< New User
oo Cameras	Email Address (Check
Detectors	
Event History	
👌 Users	
දිබු System Settings	
جې Logout	

Figure 22: New User

2. Enter the user's email and click Check to verify that the email entered is valid.

Creating Security Solutions.	USERS
Overview	USERS & PERMISSIONS FOLLOWERS
Security	 ✓ John Brown
Detectors	Personal Details:
Automation	Name * John Brown *
Event History	Email Address John@gmail.com @
	Phone Number * +445547321 Contract Add Phone
<u>S</u> Users	Country * United Kingdom of Great Britain a
င်္ဂဲွ System Settings	County / Province
🖒 Logout	City*
$\leftarrow Close$	Address *66 Croster Street
	Post Code *123435
	Security System Access: 🗸
	User Code * Check
	Show Code
	Authority Level
	Partitions * Choose partitions *
	LanguageEnglish (UK)
	Notifications Edit
	Video Devices None -
	Smart Home Devices Any
	Save Cancel Delete

Figure 23: New User Settings

- 3. Enter a user code (PIN code) one that is not assigned to another user and click Check to verify that the user code is available.
- 4. Select the required Partitions.
- 5. Select English from the language list
- 6. Define the User & Permissions settings.

- 7. For Video Devices, select from the list the video devices the user will have access to (None by default).
- 8. For Smart Home Devices, select from the list the smart home devices the user will have access to (Any by default).
- 9. Click Save to save the changes.

Add / Edit Photo

- 1. Click Add photo to add the user's photograph.
- 2. Click Browse to navigate to the photo directory and select the desired photo.





Figure 24: Add / Edit Photo

3. Click Save to save the changes.

Change Notification Settings

1. Click the Edit Notifications link to change notification settings for the current user.

Notifications	John Brown +445547321 %
All On All Off Restore Defaults	
👗 Safety	
Notify via:	
@ off	
🛕 Alarms	
Notify via:	
@ off	
👌 sos	
Save Cancel	

Figure 25: Change Notification Settings

- 2. For each type of notification, set the On/Off switch to toggle between receive or not receive emails.
- 3. Click Save to save the changes.

Editing an Existing User (Grand Master)

- 1. Click on an existing User to edit the existing user's details (see Add New User for more information).
- 2. Click Save to save the changes.

Add New CP User

1. Click Add New CP User to open the New CP User settings

RISCO creating Security Solutions.	USERS
Overview	USERS & PERMISSIONS FOLLOWERS
Security	< User1
Detectors	Personal Details:
Automation	Name * user1
Event History	Security System Access:
8 Users	User Code
දිි System Settings	Authority Level
-So Logout	Partitions * PARTITION 1 *
$\leftarrow Close$	Save Cancel Delete 🛱

Figure 26: New CP User Settings

2. Define the following CP user settings.

CP User Settings	Description	
Name	Enter the CP User's name in this field	
User Code	Enter a user code (PIN code) - one that is not assigned to another CP user - and click Check to verify that the user code is available.	
Authority Level	Select an authority level from the following:	
	• User - Arm and disarm the system; Bypass detectors; View system status, trouble and alarm event history log; Change personal user code	
	• Arm Only - Arm one or more partitions only	
	• Cleaner – A temporary code used for one-time arming in one or more partitions	
	• Duress – A special code used when coerced into disarming the system	
Partitions	Select the relevant partition(s).	

3. Click Save to save the changes.

Follower Settings

The follower setup is performed only by the Grand Master. A follower is a system user that is defined only for receiving notification messages whenever certain predefined events occur.

The Follower tab is used for defining the system follower's definitions and managing the notification definitions of each follower.



Figure 27: Follower Settings

Add New Follower

1. Click Add New Follower to open the New Follower settings.

RISCOP Creating Security Solutions Marcan	FOLLOWERS
🕂 Overview	USERS & PERMISSIONS FOLLOWERS
Security	 John De Lacross
oo □t Cameras	Personal Details:
Detectors	Name * John De Lacross
Automation	Email Address • johndela@gmail.com @ Lanouage Italian (Italy) •
Event History	
& Users	Notifications Partitions Lobby, Office *
င်္ဂြဲ System Settings	All On All Off Restore Defaults
🖒 Logout	System Status
← Close	Notify via:
	@ _ 0 7
	Save Close

Figure 28: New Follower Settings

2. Define the following follower settings.

Follower Setting	Description
Name	Enter the follower's name in this field
Email Address	Enter the follower's email address in this field
Language	Select the follower's language
Partitions	Select the partition(s) for which the current follower will receive notifications.
Notifications	Define the notification types by clicking the relevant notification type switch to toggle between On (activate) and Off (deactivate).

Editing an Existing Follower

Only the Grand Master can edit a User.

- 1. Click on an existing Follower to edit the existing follower's details (see Add New Follower for more information).
- 2. Click Save to save the changes.

System Settings Screen

Selecting the System Settings Menu displays the System Settings Screen (see below). This screen is used for editing the site details and defining date and time settings.

	SYSTEM	SETTINGS
🖄 Overview	GENERAL	
	Site Name	
		(GMT-06:00) Central Time (US & Canada)
	Country	
	County / Province	
👌 Users		
දිාරි System Settings	Address	
	Post Code	
	Phone	
	Time Format	8 42 PM (12 Hours) 20 42 (24 Hours) Cancel

Figure 29: Grand Master System Settings Screen

Creating Security Southings.	SYSTEM SETTINGS
Overview	GENERAL
Security	Time Format • 8:42 PM (12 Hours)
oO₁ Cameras	20:42 (24 Hours)
Detectors	
🖒 Automation	Cancel
Event History	
8 Users	
င်္ဂြို System Settings	
🚓 Logout	
← Close	

Figure 30: Other End Users System Settings Screen

Editing Site Details

1. Make the required changes in the fields.

RISCO Control Security Securit	SYSTEM SETTINGS	
CVerview	GENERAL	
Security	Site Name Johns Home	
Detectors	Time Zone (GMT-06.00) Central Time (US & Canada)	
🖒 Automation	Country United States of America 👻	
Event History	County / New York Province	
👌 Users		
දිටු System Settings	Address 99-05 63 Drive	
宁 Logout	Post Code	
$\leftarrow Ciose$	Phone 212 555 1212	
	Time Format	



2. Click Save to save the changes.

Date and Time Settings

1. Select the default time zone for the system and a time format (12 or 24 hrs).

	SYSTEM	SETTINGS
→ Overview	GENERAL	
Security	Site Name	
Detectors	Time Zone	(GMT-06:00) Central Time (US & Canada) 🗸 🗸
G Automation	Country	United States of America
Event History	County / Province	New York 👻
👌 Users	City	New York
දිටු System Settings	Address	99-05 63 Drive
🖒 Logout	Post Code	211345
	Phone	
	Time Format	8-42 PM (12 Hours) 20.42 (24 Hours) Cancel

Figure 32: Date & Time Settings

2. Click Save to save the changes.

Standard Limited Product Warranty

RISCO Ltd., its subsidiaries and affiliates ("**Risco**") guarantee Risco's hardware products to be free from defects in materials and workmanship when used and stored under normal conditions and in accordance with the instructions for use supplied by Risco, for a period of (i) 24 months from the date of connection to the Risco Cloud (for cloud connected products) or (ii) 24 months from production (for other products which are non-cloud connected), as the case may be (each, the "**Product Warranty Period**" respectively).

Contact with customers only. This Product Warranty is solely for the benefit of the customer who purchased the product directly from Risco, or from any authorized distributor of Risco. Nothing in this Warranty obligates Risco to accept product returns directly from end users that purchased the products for their own use from Risco's customer or from any installer of Risco, or otherwise provide warranty or other services to any such end user. Risco customer shall handle all interactions with its end users in connection with the Warranty, inter alia regarding the Warranty. Risco's customer shall make no warranties, representations, guarantees or statements to its customers or other third parties that suggest that Risco has any warranty or service obligation to, or any contractual privy with, any recipient of a product.

Return Material Authorization. In the event that a material defect in a product shall be discovered and reported during the Product Warranty Period, Risco shall, at its option, and at customer's expense, either: (i) accept return of the defective Product and repair or have repaired the defective Product, or (ii) accept return of the defective Product and provide a replacement product to the customer. The customer must obtain a Return Material Authorization ("RMA") number from Risco prior to returning any Product to Risco. The returned product must be accompanied with a detailed description of the defect discovered ("Defect Description") and must otherwise follow Risco's thencurrent RMA procedure in connection with any such return. If Risco determines in its reasonable discretion that any Product returned by customer conforms to the applicable warranty ("Non-Defective Products"), Risco will notify the customer of such determination and will return the applicable Product to customer at customer's expense. In addition, Risco may propose and assess customer a charge for testing and examination of Non-Defective Products. Entire Liability. The repair or replacement of products in accordance with this warranty shall be

Risco's entire liability and customer's sole and exclusive remedy in case a material defect in a product shall be discovered and reported as required herein. Risco's obligation and the Warranty are contingent upon the full payment by customer for such Product and upon a proven weekly testing and examination of the product functionality.

Limitations. The Product Warranty is the only warranty made by Risco with respect to the Products. The warranty is not transferable to any third party. To the maximum extent permitted by applicable law, the Product Warranty does not apply and will be void if: (i) the conditions set forth above are not met (including, but not limited to, full payment by customer for the product and a proven weekly testing and examination of the product functionality); (ii) if the Products or any part or component thereof: (a) have been subjected to improper operation or installation; (b) have been subject to neglect, abuse, willful damage, abnormal working conditions, failure to follow Risco's instructions (whether oral or in writing); (c) have been misused, altered, modified or repaired without Risco's written approval or combined with, or installed on products, or equipment of the customer or of any third party; (d) have been damaged by any factor beyond Risco's reasonable control such as, but not limited to, power failure, electric power surges, or unsuitable third party components and the interaction of software therewith or (e) any delay or other failure in performance of the product

attributable to any means of communications, provided by any third party service provider (including, but not limited to) GSM interruptions, lack of or internet outage and/or telephony failure. BATTERIES ARE EXPLICITLY EXCLUDED FROM THE WARRANTY AND RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY. Risco makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. For the sake of good order and avoidance of any doubt:

DISCLAIMER. EXCEPT FOR THE WARRANTIES SET FORTH HEREIN, RISCO AND ITS LICENSORS HEREBY DISCLAIM ALL EXPRESS, IMPLIED OR STATUTORY, REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS WITH REGARD TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND LOSS OF DATA. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RISCO AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (I) THE OPERATION OR USE OF THE PRODUCT WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE; (ii) THAT ANY FILES. CONTENT OR INFORMATION OF ANY KIND THAT MAY BE ACCESSED THROUGH THE PRODUCT BY CUSTOMER OR END USER SHALL REMAIN SECURED OR NON DAMAGED. CUSTOMER ACKNOWLEDGES THAT NEITHER RISCO NOR ITS LICENSORS CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, GSM OR OTHER MEANS OF COMMUNICATIONS AND THAT RISCO'S PRODUCTS, MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH MEANS OF COMMUNICATIONS. RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS.

RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT

IN ANY EVENT RISCO SHALL NOT BE LIABLE FOR ANY AMOUNTS REPRESENTING LOST REVENUES OR PROFITS, PUNITIVE DAMAGES, OR FOR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, EVEN IF THEY WERE FORESEEABLE OR RISCO HAS BEEN INFORMED OF THEIR POTENTIAL.

Risco does not install or integrate the product in the end user security system and is therefore not responsible for and cannot guarantee the performance of the end user security system which uses the product.

Risco does not guarantee that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection.

Customer understands that a correctly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not an assurance or a guarantee that such an event will not occur or that there will be no personal injury or property loss as a result thereof.

Consequently Risco shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning.

No employee or representative of Risco is authorized to change this warranty in any way or grant any other warranty.

Contacting your Installer / Supplier-Agent

When calling for service, ordering components, or for questions related to your camera, please contact us for assistance:

Company/agent address, phone, e-mail address:	
Contact / department:	
Hours of business:	
Website URL:	
Company logo:	
Other supplier-specific	
information:	

Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website (www.riscogroup.com) or at the following telephone and fax numbers:

United Kingdom
Tel: +44-(0)-161-655-5500
support-uk@riscogroup.com

Italy Tel: +39-02-66590054 support-it@riscogroup.com

Spain

Tel: +34-91-490-2133 support-es@riscogroup.com

France Tel: +33-164-73-28-50 support-fr@riscogroup.com **Belgium (Benelux)** Tel: +32-2522-7622 support-be@riscogroup.com

USA Tel: +1-631-719-4400 support-usa@riscogroup.com

China (Shanghai) Tel: +86-21-52-39-0066 support-cn@riscogroup.com

Israel Tel: +972-3-963-7777 support@riscogroup.com

All rights reserved.

No part of this document may be reproduced in any form without prior written permission from the publisher.

© RISCO Group 05/2019