



1. Introduction

1.1 Overview of Standard

The purpose of the Veolia Physical Security Standard is to define and provide guidance on the **Minimum** requirements to safeguard our Property and Assets.

The documents will apply the following principles to reduce the effect of those threats identified in Risk assessment.

Deter – Discourage an attempt to do something by instilling doubt or fear of consequence.

Detect – Verify and initiate an appropriate response to a threat or attack as early as possible and monitor for the loss of information or assets which have been removed

Delay – Maximising the time taken to breach our perimeter once detection has taken place.

Respond – React in an appropriate and proportionate way to prevent the loss and deter further attempts

Recover – Use our knowledge from any incidents to anticipate new vulnerabilities, threats and risks, and revisit your plans.

Any procedures, measures and investments put in place must be appropriate and proportionate for that specific situation. Every location, even within the same Region, will be different so the security requirements will change accordingly with locally identified threats and vulnerabilities. Implementing the wrong measures may prove costly, unnecessarily disruptive and may even alienate staff. Careful planning and advice will always be necessary.

2. Scope

This procedure applies to all Veolia UK & Ireland Divisions

3. Structure of Document

Section 4.1 defines the responsibilities for implementation, adherence and monitoring of the security standard.

Section 4.2 identifies the risk categories and activity examples.

Section 4.3 defines the security requirements for each identified activities. These requirements define the security measures and procedures as well as training and awareness required for **Low, Medium and High** risk security risks.

4. Standard

4.1 Responsibilities.

It is the responsibility of the Regional Director through the Line management teams to ensure that locations are meeting the minimum security requirements and in some cases exceed the requirements of this standard.

Where Veolia is not in control of a premises or activity i.e. client or contractor controlled, then it is important that Veolia assures itself that these requirements or equivalent are in place.

Assurance can be delivered through internal auditing and Director face to face engagement visits.



4.2 Risk categories and Examples.

	Veolia Risk Categories and Ratings		
Veolia Categories	Risk Rating	Definition	Examples
Veolia General	Low	Low likelihood & Low impact	Facilities that require security measures but would be unlikely to cause reputational or significant loss. I.e. Vehicle Parking areas, Transfer stations
Veolia Sensitive	Medium	High Likelihood & Low Impact	Facilities that have high value easy to access items i.e. HWRC and MRF
Veolia & Client Sensitive		Low Likelihood & High Impact	National Infrastructure type facilities that would cause reputational loss to client and Veolia. I.e. Water treatment and Energy recovery.
Critical	High	High likelihood & High impact	Activities or operations that require an extra level of security. Activities that would cause significant reputational loss to Veolia and Client and possible public safety. I.e. Secure destruction and High temperature incineration.

4.3 This section provides guidance on the level of minimum security requirements for each type of the Veolia Risk categories. These requirements define the Risks identified, Minimum security measures, Procedures and Training and awareness. Where the defined security measures requirements cannot be achieved then an equivalent must be in place based on risk assessments of any security threats.



Risks/ Threats	Low	Medium		High
	Veolia General	Veolia Sensitive	Veolia & Client Sensitive	Veolia Critical
External Theft	Site Assets Fuel IT infrastructure items	High value waste i.e. – Metals – Electricals – Batteries. Site Assets Fuel IT infrastructure items Cash on site		High value/ saleable items i.e. – Perfumes – Drugs – Commercially viable products Site Assets Fuel IT infrastructure items
Unauthorised Access	Vandalism Arson Fly tipping Injuries to Children and young people	Vandalism Arson Fly tipping Injuries to Children and young people		Vandalism Arson Fly tipping Injuries to Children and young people
Internal Theft	Waste stream Fuel Unauthorised Asset usage IT Equipment	Waste Stream High value waste i.e. Metals, Electricals, Batteries. Fuel Unauthorised Asset usage IT infrastructure items Cash on site		High value/ saleable items i.e. Perfumes, Drugs Commercially viable products Fuel Unauthorised Asset usage IT infrastructure items
Commercial competitors	Gaining information for competitive edge or espionage	Gaining information for competitive edge or espionage		Gaining information for competitive edge or espionage
Malicious People	Revenge, discredit or mischief. Abuse of staff Terrorism	Terrorism Political groups Protestors Revenge, discredit or mischief. Abuse of staff		Terrorism Political groups Protestors Revenge, discredit or mischief Abuse of staff
Reputational Loss		Loss of Reputation for Veolia and Clients		Significant Loss of Reputation for Veolia and Clients



Security Measures	Low	Medium		High
	Veolia General	Veolia Sensitive	Veolia & Client Sensitive	Veolia Critical
Access Controls	<ul style="list-style-type: none">– Access to site or building is controlled– Official identification must be carried.– Visitor passes are securely stored and the issue and return controlled Reception desk/area for Visitor Sign In– Visitors Escorted around site	<ul style="list-style-type: none">– Access to site or building is controlled– Official identification must be carried.– Visitor passes are securely stored and the issue and return controlled.– Reception desk/area for Visitor Sign In– Visitors Escorted around site		<ul style="list-style-type: none">– Access to site or building is controlled through the use of ID Cards.– Official identification must be carried and displayed at all times.– Visitor passes are securely stored and issue and return controlled.– Secure Reception desk area and Visitor Sign in during operating hours.– Visitors Escorted around site at all times – Restricted access areas identified and Access controlled.
CCTV	<ul style="list-style-type: none">– CCTV cameras and PIR monitoring at access points.– CCTV providing coverage of site during working hours– CCTV providing coverage of site during out of hours	<ul style="list-style-type: none">– Perimeter CCTV cameras and PIR monitoring – Internal CCTV Cameras and Monitoring of High risk areas.– CCTV providing coverage of site during working hours– CCTV Cameras and Monitoring when weighbridge is present.– Out of hour's notification system in place for monitoring provider.		<ul style="list-style-type: none">– Perimeter CCTV cameras and PIR monitoring – Internal CCTV Cameras and Monitoring of High risk areas.– CCTV cameras capability to monitor the entire route of High Risk waste stream– CCTV Cameras and Monitoring when weighbridge is present.– CCTV providing coverage of site during working hours– Out of hour's notification system in place for monitoring provider.



Security Measures	Low	Medium		High
	Veolia General	Veolia Sensitive	Veolia & Client Sensitive	Veolia Critical
Security Checks	<ul style="list-style-type: none">– Weekly Security Checks(Manager weekly Checks)– Yearly Security Review	<ul style="list-style-type: none">– Daily Security checks (Manager Walk round Checks) – Bi yearly Security Review		<ul style="list-style-type: none">– Random vehicle and personnel security search in place– Random drug testing for staff– Compliance with Veolia standard on ‘Disposal and Destruction of High risk Items’– Daily Security checks(Manager Walk round Checks)– Random Security/process Audit carried out by External organisation.– Site Security survey and assessment carried out by Risk and Assurance team.– Bi yearly Security Review
Manned Guarding	<ul style="list-style-type: none">– Guarding provision should be considered	<ul style="list-style-type: none">– Night Manned guarding and Patrols should be considered for Veolia & Client Sensitive facilities		<ul style="list-style-type: none">– Minimum of Night Manned guarding and Patrols– Out of hours access controlled
Storage	<ul style="list-style-type: none">– Secure storage of high value materials / tools / fuel/ IT Equipment	<ul style="list-style-type: none">– Secure storage of high value materials / tools / fuel/ IT Equipment		<ul style="list-style-type: none">– Secure storage of high value materials / tools / fuel/ IT Equipment– Restricted access areas identified and Access controlled.
General Measures	<ul style="list-style-type: none">– Site offices are lockableBoth Doors and ground level Windows– Perimeter fence > 2 meters.– External lighting (PIR detection) – Fire alarm	<ul style="list-style-type: none">– Site offices are lockable – Both Doors and ground level Windows– Perimeter fence > 2 meters.– External lighting (PIR detection)– Fire alarm and appropriate Fire protection systems – Fire alarm and evacuation routes– Lockable gates overnight		<ul style="list-style-type: none">– Site offices are lockable – Both Doors and Windows– Perimeter fence > 2 meters.– Out of hour’s notification system in place for monitoring provider.– External lighting (PIR detection)– Internal Lighting (PIR



	and appropriate Fire protection systems – Fire alarm and evacuation routes – Lockable gates overnight		detection) – Fire alarm and appropriate Fire protection systems – Fire alarm and evacuation routes – Controlled Barriers for vehicle and Pedestrian access. – Lockable gates overnight
--	---	--	--

Security Measures	Low	Medium		High
	Veolia General	Veolia Sensitive	Veolia & Client Sensitive	Veolia Critical
Procedures	<ul style="list-style-type: none"> – Staff Induction – Visitor Induction – SYS/2/027 Emergency Management Plan – SYS/2/028 Business Continuity Management – HS/2/028 Fire Safety 	<ul style="list-style-type: none"> – Staff Induction – Visitor Induction – Manned Guarding instructions – SYS/2/027 Emergency Management Plan – SYS/2/028 Business Continuity Management – HS/2/028 Fire Safety 		<ul style="list-style-type: none"> – Staff Induction – Visitor Induction – Disposal and Destruction of High risk Items’ – Manned Guarding instructions – Random Security Checks Instructions – SYS/2/027 Emergency Management Plan – SYS/2/028 Business Continuity Management – HS/2/028 Fire Safety
Training and Awareness	<ul style="list-style-type: none"> – Staff Induction – Online Security training for Line managers – Yearly Security briefing for all staff – Evacuation testing (every 6 months) 	<ul style="list-style-type: none"> – Staff Induction – Online Security training for Line managers – Yearly Security briefing for all staff – Evacuation testing (every 6 months) 		<ul style="list-style-type: none"> – Staff Induction – Online Security training for Line managers – Bi yearly Security briefing for all staff – Evacuation testing (every 6 months)
Pre Employment Checks	<ul style="list-style-type: none"> – Minimum level of checks we will: – verify identity; – confirm residency and the right to work in the UK; and – Ensure that applicants complete a self-declaration 	<ul style="list-style-type: none"> – Medium level of checks will add: – Basic criminal record disclosure – most recent academic qualifications and relevant professional qualifications; – Most recent employer reference, including dates of employment – media checks 		<ul style="list-style-type: none"> – High level of checks will add: – criminal record disclosure if relevant to the – all academic and professional qualifications; – employment references – basic confirmation with



	criminal record form.		employers of dates of employment, posts held and reasons for leaving, and line manager references (if possible); – media checks; – financial enquiries
--	-----------------------	--	--