BUILT ASSET SECURITY STRATEGY

Name of Built Asset

For the purposes of this Strategy, the *Name of Built Asset* encompasses:

-

For the purposes of this Strategy, neighbouring built assets are:

-

The data and information that is classed as sensitive is that pertaining to:

Legislation, Standards and Codes of Practice relevant to the built asset are:

Document	**Date/Version**

BUILT ASSET RISK MANAGEMENT STRATEGY

RISK ASSESSMENT

Threat agent	Motivation	Period in lifecycle of asset where threat may act	Potential action(s) of the threat agent
T1	**M1**		Hostile reconnaissance
			Hostile reconnaissance
T2			Hostile reconnaissance
			Hostile reconnaissance
T3			Hostile reconnaissance

Summary of potential actions:

Potential action	Threat agent that may utilise action[1]			Period in lifecycle						
	T1	T2	T3	Planning	Tendering	Design	Construction (incl. major improvement & modification)	Ongoing maintenance and management	Minor improvement & modification	Disposal
A1 Hostile reconnaissance	✓	✓✓	✓							

[1] The number of ticks indicates the number of motivations of the threat agent to which the potential action is relevant

For each of the potential actions of the threat agents, the vulnerabilities that could be exploited are:

Potential action	Potential vulnerabilities
A1 Hostile reconnaissance	

Summary of potential vulnerabilities against potential actions

Potential vulnerability	Potential actions						
	A1	A2	A3	A4	A5	A6	A7
V1							

Summary of potential vulnerabilities

Potential vulnerability	Threat agent that may utilise vulnerability[2]		
	T1	T2	T3
V1			

[2] The number of ticks indicates the number of motivations of the threat agent to which the potential vulnerability is relevant

Summary of the vulnerabilities and potential impacts if exploited by a threat(s):

Ref.	Motivation that vulnerability could be exploited to help achieve	Compromise of, or harm caused to:	Impact of compromise or harm
V1	**M1**	E.g. Personnel and other users of the asset The built asset itself The services delivered from the built asset Personal data	E.g. Injury or harm caused to personnel Damage caused to the built asset Disruption of, or interruption to, service Inconvenience, delay and disruption to the wider aspects of the work of the organisation Breach of privacy Financial damage Reputational damage Compromise of national security

The risk associated with the potential of each vulnerability being utilised by a threat agent:

Ref.	Motivation	Likelihood	Severity of impact	Resultant risk	Risk ref.	Notes
V1	**M1**				R1.1	
					R1.2	
					R1.3	
					R1.4	
					R1.5	

RISK MITIGATION

For any risks that are not acceptable, the potential mitigation measures are:

Risk Ref.	Mitigation measures	Mitigation ref.
R1.1 – 1.5		R1.M1
		R1.M2
		R1.M3

The assessment of each potential mitigation, is set out in the table below:

Mitigation ref.	Risk with measure in place		
	Likelihood	Severity	Risk
R1.M1 – M3			

Mitigation measures to be implemented:

Mitigation ref.	Description	Measure to be implemented?	If measure not to be implemented, record reasons
R1.M1			
R1.M2			
R1.M3			

List of those to be informed of residual risks:

Details of when the will BASS be reviewed (including ad-hoc reviews)?

Those positions authorised to conducted a review are:

A review is to be undertaken after a trigger event within:

The timescale from completing a review is:

The timescale for updating the BASS, when a review finds this to be necessary, is:

The process for re-issue of the BASS and removal of the redundant version is:

Copies of all reviews should be stored in an Appendix to the BASS

This document should be signed by an appropriate senior manager within the asset owner's organisation.

Signature	Date