**Table of Policies**

## DEFINITIONS

For the purposes of this document, the following definitions, consistent with those contained in PAS 1192-5:2015, apply:

### Asset Information

Information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organisation.

*NOTE: Asset information includes design information and models, documents, images, software, spatial information and task or activity-related information.*

### Asset Data

Data relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organisation.

### Built Asset

Building, multiple buildings (e.g. a site or campus) or built infrastructure (e.g. roads, railways, pipelines, dams, docks, etc.) that is the subject of a construction project or where the asset information is held in a digital format.

*NOTE: The built asset may include associated land or water, for example, the catchment area for a water company or the navigation channels for a dock. It may also comprise a portfolio or network of assets.*

### Level of Definition

Collective term used for and including "level of detail" and the "level of information".

## ACRONYMS

| | |
|---|---|
| **BASIR** | Built Asset Security Information Requirements |
| **BASM** | Built Asset Security Manager |
| **BASMP** | Built Asset Security Management Plan |
| **BASS** | Built Asset Security Strategy |
| **SB/IMP** | Security Breach/Incident Management Plan |

## 1 CHECKING ASSET INFORMATION

Impact on other areas/security specialisms

| **Impact on other areas/security specialisms (highlighted fields)** | | |
|---|---|---|
| HR | Physical | Technological |

### 1.1 Mitigation References

-
-

### 1.2 Policy

1.2.1 E.g. *Checks shall be in place to ensure that whenever asset information, including that pertaining to neighbouring sensitive assets, is sent to an individual or an organisation, it shall not contain that to which an individual or organisation has not been granted access.*

### 1.3 Related Policies

1.3.1 This policy is reliant on the following policies also being in place:

-
-
-
-

1.3.2 If any of the above are altered, this policy shall be reviewed and any necessary alterations made to it in order to ensure essential risk mitigation measures remain in force.

1.3.3 The following policies are dependent on this policy being in place:

-
-
-
-

1.3.4 If this policy is altered, each of the above shall be reviewed and any necessary alterations made to them in order to ensure essential risk mitigation measures remain in force.

1.3.5 Role responsible:

-

### 1.4 Supporting Processes

1.4.1

1.4.2 Roles responsible:

-
-
-

## 1.5 Monitoring and Auditing of Policy

1.5.1 Implementation of this policy shall be monitored and audited by:

- X
- Y

1.5.2 The supply chain shall collaborate with, and support, the X and Y in the monitoring and auditing process.

## 2

| Impact on other areas/security specialisms (highlighted fields) | | |
|---|---|---|
| HR | Physical | Technological |

### 2.1 Mitigation References

-
-

### 2.2 Policy

2.2.1

### 2.3 Related Policies

2.3.1 This policy is reliant on the following policies also being in place:

-
-
-

2.3.2 If any of the above are altered, this policy shall be reviewed and any necessary alterations made to it in order to ensure essential risk mitigation measures remain in force.

2.3.3 The following policies are dependent on this policy being in place:

-
-
-

2.3.4 If this policy is altered, each of the above shall be reviewed and any necessary alterations made to them in order to ensure essential risk mitigation measures remain in force.

2.3.5 Role responsible:

-

### 2.4 Supporting Processes

2.4.1

2.4.1.1 Roles responsible:

-

### 2.5 Monitoring and Auditing of Policy

2.5.1 Implementation of this policy will be monitored and audited by:

- X
- Y

2.5.2 The supply chain shall collaborate with, and support, X and Y in the monitoring and auditing process.