Bilsington Parish Council

Information Risk Management Policy

1. **Aim**
    1. The aim of this policy is to set out Bilsington Parish Council's approach to information risk management.
2. **The Purpose of Information Risk Management**
    1. Information Risk Management is a key element of information assurance and the corporate governance of an organisation. It ensures risks are considered against organisational benefits and assists in exploiting information opportunities whilst maintaining confidence and reassurance that risks are appropriately managed.
3. **Identifying Information Risk**
    1. Bilsington Parish Council uses various internal and external sources to identify information risks including:
        1. Local threat assessment;
        2. Monitoring compliance with Information Security Management System;
        3. National advice and guidance;
        4. Security incident reporting;
        5. Technical and procedural failures;
        6. Change management;
        7. Information Technology Health Checks / Penetration testing;
        8. External statutory and regulatory obligations;
        9. Policy exceptions.
4. **Assessing Risk**
    1. A qualitative risk assessment, based on the corporate risk approach is used to assess the probability of an event happening and the impact should it happen.
    2. Confidentiality, integrity or availability of the assets form part of the assessment.
    3. A scale of 1 – 4 for likelihood and impact is used in line with the corporate risk model.
5. **Treatment of Information Risk**
    1. Bilsington Parish Council address information risk using four key aspects of Information Risk Management internal control:
        1. Tolerate – the decision on retaining the risk without further action.
        2. Treat – the decision to introduce, remove or alter controls so that the residual risk can be reassessed as being acceptable. This must be achieved through the following actions:
            a. Preventative – stop undesirable events happening e.g. limiting action to an authorised person;
            b. Corrective – restore normality after the occurrence of undesirable events e.g. business continuity planning;
            c. Directive – encourage desired behaviour or outcomes e.g. training staff; and
            d. Detective – detect the occurrence of undesirable events e.g. audit and monitoring.
        3. Transfer – the decision to transfer the risk to another party in order to manage the risk more effectively. Reputational risk cannot be transferred.
        4. Terminate – the decision to avoid the risk completely by withdrawing from a planned or existing activity or set of activities.
6. **Monitoring Information Risk**
    1. Risks and their factors will be monitored and reviewed:

1. Context – identifying changes to underlying assumptions or new factors.
2. Controls – ensuring the controls for risks do not become less effective or irrelevant.
3. Treatments – ensuring risk treatments are appropriately implemented and maintained.

7. Recording Information Risk

1. Information Risk Register

1. An Information Risk Register will be maintained and will act as a central repository for high level information risks. The Information Risk Register will be available at all times to those involved in the risk process.

2. Risk Balance Case

1. A Risk Balance Case approach has been adopted to capture information risks created as a result of policy exceptions

3. Information Security Management System Risk Register

1. A risk register holding risks specific to the management of the information security management system and related controls will be maintained.

8. Shared Risk

1. Bilsington Parish Council recognise that ownership of information risk can be shared and the impact can therefore be external to Bilsington Parish Council, for example through partnership working.
2. Bilsington Parish Council will work with its partners to ensure risks are managed and communicated to ensure organisations can discharge their responsibilities appropriately.

9. Risk Appetite Levels

1. Taking into account the internal and external factors the risk appetite for information risks is **Cautious.**
2. The following table presents the corporate risk appetite levels.

Appetite Levels	Description
Averse	Preference for safe business delivery options that have a low degree of inherent risk and only a potential for limited reward. Low risk options taken to minimise exposure – reluctant to take action given uncertainty – highly influenced by experience.
Cautious	Preference for safe delivery options that have a medium degree of residual risk and may only have limited potential for reward. 'willing to take risks but prefer to take the 'safe delivery option' – minimising the exposure with tight corporate controls over change'
Creative and Aware	Wiling to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing a good level of reward. 'no surprises – well measure risk taking – willing to take risk with a degree of uncertainty – recognising things will go wrong – learn from mistakes'

Hungry	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk. Recognise highly developed decision making – will mean that not all risks are known – take action when uncertain of results or with uncertain info – willing to accept significant loss (money/reputation) for higher potential reward’