# IT Risk Management Policy

| | |
|---|---|
| Organisation | National Film and Television School |
| Title | IT Risk Management Policy |
| Creator | Director of Operations |
| Approvals Required | 1. Head of IT 2. Director of Operations 3. Management Team |
| Version | Version 1 |
| Owner | Director of Operations |
| Subject | The formal approved IT risk management policy of NFTS |
| Rights | Public |
| Review date and responsibility | Annually by Head of IT/Director of Operations |

| Document Amendment History | | |
|---|---|---|
| v0.1 | Draft IT Risk Management Policy | Feb 2017 |
| V0.2 | With management feedback | March 2017 |
| v1.0 | Finalising policy following Management Team meeting | June 2017 |

# 1. Introduction

In addition to the NFTS risk management policy, which forms part of the School's internal control and corporate governance arrangements, the National Film and Television School (NFTS) shall conduct ongoing assessments of threats and risks related to information assets, to determine the necessity of safeguards, countermeasures and controls.

In the NFTS risk management policy the NFTS shall be considered to be averse to IT risk.

The NFTS shall continuously monitor for any change in the threat environment and make any adjustment necessary to maintain an acceptable level of risk. The NFTS risk management process Includes:

- Identifying key information assets and subjecting them to IT specific risk assessments
- Identifying level of compliance to Industry best practice for risk management and Information Security
- Assessing exposure to a list of common threats and vulnerabilities
- Maintaining risk registers, which include information security and operational risks
- Implementing technical, policy, Business Continuity and Management initiatives to reduce or eliminate identified risks.
- Regular reviews of the performance and effectiveness of implemented controls
- Reporting significant risks to the NFTS Management Team through the Director of Operations.

NFTS have implemented a formal IT Risk Management process to identify and manage security and operational risks, and apply appropriate management action. The basic approach that has been adopted for assessing the risks is based on the following key activities:

- Asset and Risk Identification
- Business Impact Assessment
- Risk Assessment
- Identifying the threats and vulnerabilities related to these assets
- Calculating the resulting risk exposure and impact
- Agreeing controls, activities and processes to treat risks
- Implementing risk treatment initiatives and controls

Regular reviews of the asset list and the business risk profile are part of the risk assessment approach for information security in particular aligned with ISO/IEC 27001:2013. This enables compliance with the policy to be checked as well as the ongoing effectiveness of the implemented controls.

# 2. Asset and Risk Identification

Information Assets and risks to operations will be identified during meetings and interviews with key business managers and process owners within NFTS. The Head of IT or his/her team documents the assets within an information asset list or risk register. Where possible / appropriate, information assets are grouped together to simplify the management of the risk and compliance.

The asset list shall contain as a minimum:

- A name and description of the asset / risk
- The physical and/or logical location of the asset. This may include an application or system
- The type of asset / risk
- The employee / interviewee that described the asset
- The Owner of the asset / asset group

# 3. Asset Owners

Owners of the Assets / asset groups are identified and documented in the asset/risk register. The owner is defined as an individual with overall responsibility for ensuring appropriate security and control is applied to the assets.

Note:

The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ’owner’ does not mean that the person actually has any property rights to the asset. (Extract from ISO27001:2005).

# 4. Business Impact Assessment

In identifying the list of risks to IT services, what is important for the NFTS is the degree and severity of the impact of that service failing or operating at a non-optimised level. The NFTS approach to risk will ensure that full analysis is made of the potential impact to the School of these risks being realised.

# 5. Risk Assessment

The current state of the organisation is assessed against each risk / threat, based on information from the interviews and assessment, specific risk assessment meetings, and information obtained in the risk assessment process.

The Risk Assessment calculates the overall risk value to the asset / groups, and details a risk rating to help the organisation identify high risks and exposures. Appropriate management action must then be taken to assess the appropriate action to mitigate the risk, or to accept, transfer or avoid the risk.

The Risk register will be made available (if appropriate) by request to IT@nfts.co.uk

## 5.1 Measurement of Risk

NFTS uses a straightforward combination of impact and likelihood to judge the overall level of risk

To enable NFTS to prioritise the mitigations to threats to their interests, the Head of IT and Director of Operations together with subject matter experts are empowered to rate the importance of the threat in accordance with the following table.

### 5.1.1 Impact Assessment

| Threat Level | Rating Description |
|---|---|
| 1-2 Low | The likelihood of the threat affecting the business is low, as this threat is not relevant to this business or industry, or is not relevant to the business functions, or has a historically low track record of exploit or vulnerability. |
| 3-4 Med | The likelihood of the threat affecting the business is medium, as this threat may be relevant to this business or industry, or has some relevance to the business functions, or there is some historical and industry evidence of exploit and threat. |
| 5 High | The likelihood of the threat affecting the business is high, as this threat is very relevant to this business or industry, or has direct relevance to the business functions, or there is significant historical and industry evidence of exploit and threat. |

The risk Assessment shall detail the threat value for each risk, or for a group of risks.

### 5.1.2 Likelihood Assessment

For each threat, the organisations' current and literal exposure is assessed, based on the controls currently in place, information obtained from interviews, knowledge

of the business and processes, to determine the potential impact to the School if the risk/threat were realised.

The Head of IT and Director of Operations along with subject matter experts will select a likelihood rating for each risk based on the following table:

| Rating | |
|---|---|
| 5-Very High | It is almost certain that the vulnerabilities will be exploited as there are no controls in place or it has happened in the past |
| 4 High | It is highly possible that the vulnerabilities will be exploited. as there is little or no protection in place |
| 4 Medium | It is possible that the vulnerabilities will be exploited as some protection is in place |
| 2 Low | It is unlikely that the vulnerabilities addressed will exploited as the protection in place is considered to be good |
| 1 Very Low | It is improbable that the vulnerabilities will be exploited as the controls in place are considered to offer excellent protection |

The Risk Assessment shall detail the organisations vulnerability value for each threat.

### 5.1.3 Risk Analysis

The risk measure is calculated by multiplying the impact value of the asset / asset group by the likelihood of the risk happening. To calculate the Risk Measure the following calculation is performed:

Likelihood x Impact = Risk Measure

The resulting number can be used to create a Risk Measure, which can then be rated as Very Low, Low, Medium, High and Very High Risk and treated accordingly.

### 5.1.4 Risk Management Scale

In order to identify the identify risk management options, risks management options will be defined as High, Medium, or Low according to the predefined table below:

| Rating | Risk Measure | Rating Description |
|---|---|---|
| LOW | 0-9 | The low level of risk does not justify additional controls being put in place. No further activity necessary. |
| MEDIUM | 10-16 | Management will apply their judgement as to whether or not the risks are acceptable. Controls will be applied as appropriate. |
| HIGH | 17-25 | Management will select appropriate controls as a priority |

**The Risk Assessment shall detail the resulting Risk Value for each identified theme.**

# 6. Risk Treatment

All risks that result in a LOW or VERY LOW risk measure shall automatically be accepted and no further action shall be required.

All Risks that result in a MEDIUM, HIGH or VERY HIGH shall be reviewed for further management action. The Head of IT shall review all such risks with the Director of Operations and the Asset Owners to decide an appropriate risk treatment action.

Risks measured as High will result in a business case being made to the School's investment governance board with the range of options to remove, reduce or mitigate the risk. Thus the decision on which risks are acceptable, or not, will ultimately be made by the School's management team.

# 7. Risk Treatment Plan

The Head of IT is responsible for establishing and maintaining the risk treatment plan in order to achieve the identified control objectives. The Risk Treatment Plan details the following:

- The source of the Risk, threat and vulnerability from the risk assessment
- The Asset(s) at risk if applicable
- The owner of the Risk
- The proposed management action (Reduce, Accept, Avoid, Transfer)
- The proposed controls and actions to be carried out to REDUCE risks
- The proposed timescale and deadlines for completion of the proposed actions

The risk treatment plan shall identify priorities based upon the perceived risk, and considers funding, responsibilities, actions and estimated date of completion.

The Head of IT is responsible for tracking and chasing the progress of risk treatments, and updating the Risk Treatment Plan with progress and updated actions.

The Head of IT and Director of Operations will review the Risk Treatment Plan regularly (at leat 4 times per year) and ensure that actions are being implemented and closed in a timely manner. If required, the Director of Operations will escalate unresolved or slow actions to the appropriate management functions to ensure actions are dealt with.

# 8. Ongoing Risk Management

The ongoing management of risks is controlled by assessing data from incident reports, audit results, technical advisories and confirmed or potential technical or process vulnerabilities and if required creating subsequent risk assessments. New critical information assets, processing facilities and buildings are subjected to risk assessment as part of the project process.

The Head of IT is responsible for ensuring that changes to NFTS, its technology, business objectives, processes, legal requirements and identified threats are incorporated into the Risk Assessment and Management process. Where appropriate the Head of IT will initiate a risk assessment process to ensure that security controls are relevant. The risk assessment shall follow the same assessment process detailed in this document.

NFTS can if required reactively implement additional controls without undertaking a full risk assessment, if the threat or vulnerability could have a significant impact on NFTS, its partners or personnel.