Standard Operating Procedures (SOP) for:			
Information Risk Assessments			
SOP Number:	**DG01**	Version Number:	**1.3**
Effective Date:	**15 July 2014**	Review Date:	**14/07/2015**

Author: Reviewer:	**William Mordaunt, IT Services Project Manager** **Shelim Miah, Risk & Governance Manager**

Authorisation:	
Name / Position	**Chris Day, Director of IT Services**
Signature	**C Day**
Date	**15 July 2014**

Accountability:	
Position	Line Managers
Responsibility:	
Position	Directors/ Heads of Department Risk Assessors

Revision History			
Version	Description	Author	Date
1	Initial version.	William Mordaunt	16/08/2010
2	Revised to align with College risk system.	William Mordaunt	16/08/2011
2	Annual Review – No Change	Shelim Miah	14/07/2014

Purpose and Objective:

To ensure that all information risk assessments are performed in a systematic and rigorous manner.

To define a systematic approach for conducting information risk assessments.

This procedure is based on the Queen Mary Risk Management Strategy, adjusted to suit information security risks.

References:

QM Risk Management Strategy

SOP Text

	Responsibility	Activity
1.	Directors/ Heads of Department	Each Director/Head of Department shall assign responsibility for conducting an information risk assessment to a suitably senior person.
2.	Risk Assessor	Identify information assets within the scope of the risk assessment and their owners (roles not names). Record the assets on the Information Risk Assessment worksheet

		(Appendix A).
3.	Risk Assessor	Identify the criticality of each asset. Prioritise the risk assessment by addressing the more critical assets first.
4.	Risk Assessor	For each asset identified, identify the threats to and vulnerabilities of the asset. Record these on the worksheet. Identify whether each threat or vulnerability impacts the confidentiality, integrity, or availability of the asset.
5.	Risk Assessor	Identify impacts. Assess the impact on the organisation of a compromise of confidentiality, integrity, and availability for each asset and enter the corresponding impact score onto the worksheet. Use the table in Appendix B as a guide to assess the extent of loss for each impact. For example, an event that resulted in a loss of service for more than 1 day but less than 1 week would be rated as Minor with an impact score of 2.
6.	Risk Assessor	Assess the likelihood or probability of each impact and enter the corresponding probability score onto the worksheet. Use the table in Appendix C as a guide to assess the probability of each impact. An event that occurs, or is likely to occur, at least once a week would be rated as Almost Certain with a probability score of 5.
7.	Risk Assessor	The worksheet will calculate a risk rating by multiplying the impact score by the probability score as illustrated in Appendix D.
8.	Risk Assessor	The output from the risk assessment should then be used as the basis for a risk treatment plan. The items with the risk rating of High should be addressed as a priority.

List of appendices

Appendix	Appendix name	Location
Appendix A	Information Risk Assessment Worksheet	Accompanying MS Excel spreadsheet
Appendix B	Impact Scoring	On page 3
Appendix C	Probability Scoring	On page 4
Appendix D	Mapping of Risk Scores to Risk Ratings	On page 5

Appendix B – Impact Scoring

Impact Rating	Extent of the possible loss for each potential impact	Impact Score
Negligible	Minor injury/illness requiring first aid Loss of service for less than 8 hours No media interest	1
Minor	Injury/illness requiring more than 3 days absence from work Loss of service for more than 1 day Potential for adverse publicity	2
Moderate	Injury/illness requiring major clinical intervention Loss of service for more than 1 week Probable media interest	3
Major	Incident causing permanent injury or death Loss of service for more than 1 month Media interest and adverse publicity	4
Catastrophic	Incident causing multiple permanent injuries or deaths Permanent loss of service or facility Extensive media interest and adverse publicity Financial viability of the organization is threatened	5

Appendix C – Probability Scoring

Probability Rating	Probability of each impact occurring	Probability Score
Rare	Up to 2% likely to happen or a one in fifty chance; likely to occur less frequently than once per year	1
Unlikely	Up to 5% likely to happen or a one in twenty chance; likely to occur more than once every year but less than once every six months	2
Possible	Up to 10% likely to happen or a one in ten chance; likely to occur more than once every six months but less than once every month	3
Likely	Up to 20% likely to happen or a one in five chance; likely to occur more than once every month but less than once every week	4
Almost Certain	At least 50% or a one in two chance or more likely to happen than not; likely to occur at least once every week	5

Appendix D – Mapping of Risk Score to Risk Ratings

Likelihood	5 – Almost certain	5	10	15	20	25
	4 – Likely	4	8	12	16	20
	3 – Possible	3	6	9	12	15
	2 – Unlikely	2	4	6	8	10
	1 – Rare	1	2	3	4	5
		1 Neg	2 Min	3 Mod	4 Maj	5 Cat
	Impact					

Risk Score	**Risk Rating**
0 – 6.9	Low
7 – 13.9	Medium
14– 25	High