Ipsos MORI

Information Security Policy

Information is the main product produced by Ipsos MORI. It's therefore vital that the information we use is kept secure from accidental or deliberate loss, destruction or disclosure. It is also essential that information is accurate, complete and available when its needed. As a result, the board and management of Ipsos MORI are committed to the effective management and security of information. In support of this commitment, the Management Board have put in place appropriate information security policies, procedures and processes as a central element of our integrated quality, compliance and information security management system – our "Business Excellence System".

This policy, together with the other policies, procedures and processes that implement our Business Excellence System apply to all employees, casual workers, interviewers and contractors engaged by Ipsos MORI, collectively our "staff", as well as anyone visiting our offices. Any member of staff failing to comply with the requirements of our information security policies, procedures and processes will be subject to appropriate disciplinary action. A deliberate breach by anyone may also constitute an offence under The Computer Misuse Act 1990 and/or The Data Protection Act 1998.

Objectives

The core information security objective of our Business Excellence System is to ensure the proper and effective management of information throughout the organisation in order to fully support our corporate objectives. Our Business Excellence System will achieve this by:

- providing assurance that we collect and process information in compliance with our legal, contractual and industry code of practice obligations;
- assisting the business in retaining existing clients and gaining new business by having effective policies, procedures and practices in place for the appropriate security of information;
- minimising damage to the business in the event of any breach of information security; and
- helping to ensure business continuity in the event of a disaster.

Our approach to information security:

Ipsos MORI will:

- Use all reasonable, appropriate, practical and effective measures to protect our premises, equipment, processes and information – our information "assets" - in order to achieve our information security objectives.
- Ensure its information security policies, procedures and processes that form part of our integrated management system meet the requirements of the international standard for information security, ISO 27001.
- Continually review and improve its information security measures to ensure they continue to effectively support the business and remain compliant with our legal, regulatory and contractual obligations.

Responsibilities for information security:

The overall direction and leadership of Information security and our Business Excellence System will be provided by "the Ipsos MORI Information Governance forum", a sub-committee of the UK Management Board. The Forum will meet at least bi-annually, with additional meetings as required in response to major business changes, security threats or breaches.

The Head of Compliance and Information Security is responsible for the operational management of Information Security.

Everyone is responsible for ensuring they comply with our information security policies, procedures and processes in order to maintain the confidentiality, accuracy, integrity and availability of the information we collect, process, store and hold in trust from our clients and respondents. All staff with management or supervisory responsibilities are also responsible to the Board for actively promoting best practice amongst their staff and for ensuring their staff comply with the company's integrated management system's policies, procedures and processes relevant to the areas they manage or supervise.

Information risk management:

The management of information risk is essential to ensuring we meet our business and information security objectives. Our planning and implementation of information risk management is detailed in our documented approach to risk, which requires all information and information processing equipment and systems – "information assets" - to be recorded in a log, together with details of the manager or supervisor responsible for the items recorded. The information assets recorded in the log will then be managed in accordance with an initial risk assessment. Following this, regular risk reviews will take place.

Risk assessments consider current and potential threats, the information asset's vulnerability to those threats, the likelihood of occurrence and the impact on the business should it occur. Risk assessments will be reviewed if any significant change to the information asset occurs, new threats to the asset are identified or at least annually as appropriate.

It is the responsibility of the manager responsible for the information "asset" to ensure a risk assessment is carried out in the event of any new information processing facilities, types of business, information or information processing measures being introduced. Risk assessments will also be reviewed in response to any other significant changes to the information, information processing or the legal, regulatory, contractual or social landscape.

The Head of Compliance and Information Security is responsible for the operational implementation of information risk management.

Implementation of Information Security:

This policy is implemented by the information security policies, procedures and processes that form part of our make up our integrated quality, compliance and information security management system.

Reporting Information Security Breaches:

Any information security incident must be reported to the Compliance & Information Security Department immediately it occurs or is discovered in line with our Information Security Incident Reporting and Management procedures.

Authorised by: Ben Page, Chief Executive.

Ipsos MORI

Information Security Policy

Information is the main product produced by Ipsos MORI. It's therefore vital that the information we use is kept secure from accidental or deliberate loss, destruction or disclosure. It is also essential that information is accurate, complete and available when its needed. As a result, the board and management of Ipsos MORI are committed to the effective management and security of information. In support of this commitment, the Management Board have put in place appropriate information security policies, procedures and processes as a central element of our integrated quality, compliance and information security management system – our "Business Excellence System".

This policy, together with the other policies, procedures and processes that implement our Business Excellence System apply to all employees, casual workers, interviewers and contractors engaged by Ipsos MORI, collectively our "staff", as well as anyone visiting our offices. Any member of staff failing to comply with the requirements of our information security policies, procedures and processes will be subject to appropriate disciplinary action. A deliberate breach by anyone may also constitute an offence under The Computer Misuse Act 1990 and/or The Data Protection Act 1998.

Objectives

The core information security objective of our Business Excellence System is to ensure the proper and effective management of information throughout the organisation in order to fully support our corporate objectives. Our Business Excellence System will achieve this by:

- providing assurance that we collect and process information in compliance with our legal, contractual and industry code of practice obligations;
- assisting the business in retaining existing clients and gaining new business by having effective policies, procedures and practices in place for the appropriate security of information;
- minimising damage to the business in the event of any breach of information security; and
- helping to ensure business continuity in the event of a disaster.

Our approach to information security:

Ipsos MORI will:

- Use all reasonable, appropriate, practical and effective measures to protect our premises, equipment, processes and information – our information "assets" - in order to achieve our information security objectives.
- Ensure its information security policies, procedures and processes that form part of our integrated management system meet the requirements of the international standard for information security, ISO 27001.
- Continually review and improve its information security measures to ensure they continue to effectively support the business and remain compliant with our legal, regulatory and contractual obligations.

Responsibilities for information security:

The overall direction and leadership of Information security and our Business Excellence System will be provided by "the Ipsos MORI Information Governance forum", a sub-committee of the UK Management Board. The Forum will meet at least bi-annually, with additional meetings as required in response to major business changes, security threats or breaches.

The Head of Compliance and Information Security is responsible for the operational management of Information Security.

Everyone is responsible for ensuring they comply with our information security policies, procedures and processes in order to maintain the confidentiality, accuracy, integrity and availability of the information we collect, process, store and hold in trust from our clients and respondents. All staff with management or supervisory responsibilities are also responsible to the Board for actively promoting best practice amongst their staff and for ensuring their staff comply with the company's integrated management system's policies, procedures and processes relevant to the areas they manage or supervise.

Information risk management:

The management of information risk is essential to ensuring we meet our business and information security objectives. Our planning and implementation of information risk management is detailed in our documented approach to risk, which requires all information and information processing equipment and systems – "information assets" - to be recorded in a log, together with details of the manager or supervisor responsible for the items recorded. The information assets recorded in the log will then be managed in accordance with an initial risk assessment. Following this, regular risk reviews will take place.

Risk assessments consider current and potential threats, the information asset's vulnerability to those threats, the likelihood of occurrence and the impact on the business should it occur. Risk assessments will be reviewed if any significant change to the information asset occurs, new threats to the asset are identified or at least annually as appropriate.

It is the responsibility of the manager responsible for the information "asset" to ensure a risk assessment is carried out in the event of any new information processing facilities, types of business, information or information processing measures being introduced. Risk assessments will also be reviewed in response to any other significant changes to the information, information processing or the legal, regulatory, contractual or social landscape.

The Head of Compliance and Information Security is responsible for the operational implementation of information risk management.

Implementation of Information Security:

This policy is implemented by the information security policies, procedures and processes that form part of our make up our integrated quality, compliance and information security management system.

Reporting Information Security Breaches:

Any information security incident must be reported to the Compliance & Information Security Department immediately it occurs or is discovered in line with our Information Security Incident Reporting and Management procedures.

Authorised by: Ben Page, Chief Executive.