WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Business Continuity (ISP)**
POLICY REFERENCE NO:	**Inf/16**

Executive Summary.

In accordance with the HMG SPF Risk Management West Midlands Police will ensure that appropriate security measures are implemented and managed to control access to information assets and reduce the risks associated with unauthorised system access and information disclosure.

Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.

Intended Policy Audience.

This policy applies to every police officer, member of police staff, police community support officer, special constable, volunteer, contractor, and approved persons working for or on behalf of West Midlands Police.

Current Version And Effective Date.	**Version 0.2**	**14/01/2015**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Paul Richards – Information Security Officer**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**10/02/2015**	
Review Date	**10/02/2016**	
Protective Marking	**Not Protectively Marked**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- HMG Security Policy Framework (SPF);
- CESG IA Standards (IAS) and Good Practice Guides (GPG's);
- BS ISO27001:2013 – Information Technology
- Security Assessment for Protectively Marked Assets (SAPMA)
- WMP Local Threat Assessment
- Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Diversity Vision Statement and Values

"Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values"

"All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay."

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organization to do the right thing.

CONTENTS

1.   INTRODUCTION.

1.1.   The Chief Constable of West Midlands Police is a Category 1 Responder as defined by the Civil Contingencies Act 2004 (CCA) and has duty to maintain plans to ensure that they can continue to perform their functions in the event of an Emergency, so far as is reasonably practicable. This duty relates to all the functions of a Police Force, not just its civil protection functions.

1.2.   The Chief Constable, as part of the 'Tri-Partite' arrangements responsible for the provision of an efficient and effective police service in West Midlands has a wide range of statutory and other duties and responsibilities. The staff and other resources employed by or on behalf of West Midlands Police perform functions intended to enable the Chief Constable to meet their responsibilities.

1.3.   West Midlands Police will strive to meet all the business continuity related duties placed upon it by the CCA and will develop, maintain and implement plans that ensure the Force is able to continue to perform its functions so far as is reasonably practicable in the event of a range of disruptive challenges.

1.4.   West Midlands Police will seek to adopt good practice as described within the statutory and non-statutory guidance issued under the CCA and by authoritative bodies such as Cabinet Office and HMIC.

2.   BUSINESS CONTINUITY POLICY

Overview

2.1.   In relation to Business Continuity Management (BCM) the Force will adopt the principles described within British Standards Institutes - ISO 22301 which specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents.

2.2.   This policy is applicable to the whole Force and, where required in contracts, to persons or organisations contracted to provide goods and services on behalf of the Force.

2.3.   The scope of activities to be subjected to BCM processes will be limited. The Assistant Chief Constable (Protective Services) as chair of a Force Resilience Forum will be responsible for determining the scope of BCM by identifying the most important and time sensitive objectives for West Midlands Police to which BCM methodology should be applied as a risk control measure. The specified objectives will define which activities enable delivery of the key products and services that support achievement of the objectives (these will be called Critical Activities).

2.4.   Risks relating to activities not covered by this Policy will be managed by alternative means. All risks relating to Critical Activities with a 'maximum tolerable period of disruption' of greater than 90 days will be dealt with under arrangements imposed by the generic Force Risk Management Policy. It is also expected that some risks initially identified by processes supporting the Force Risk Management Policy may need to be referred for Business Continuity Management processes to be applied.

The aim of the policy

2.5.	To ensure the Chief Constable meets their statutory responsibilities relating to Business Continuity imposed by the Civil Contingencies Act 2004 and is able to continue to perform their functions in the face of reasonably foreseeable disruptive challenges.

General Principles of the Policy

2.6.	The Business Continuity Management objectives of West Midlands Police will be:

- Identify and agree a list of the Critical Activities completed by the force (including those undertaken by other persons or agencies on behalf of the force) which enable West Midlands Police to meet its most important and time sensitive objectives.
- Produce and maintain appropriate performance measures and guidelines regarding acceptable minimum standards of performance related to Critical Activities.
- Agree the maximum tolerable period of disruption for each Critical Activity.
- Produce plans which will ensure Critical Activities can be maintained or recovered to acceptable minimum standards within the agreed maximum tolerable period of disruption for each activity.
- To indicate recommended alternative loss mitigation or risk treatment measures that should be applied to remaining identified risks.
- The Assistant Chief Constable (Protective Services) will be responsible for implementation, development and review of this Policy. The Policy will be reviewed at least every 2 years or sooner if required. They will appoint persons as appropriate to a Force Resilience Forum. This 'Forum' will be responsible for:
- Implementing business continuity arrangements within the Force.
- Overseeing implementation and maintenance of BCM arrangements.
- Approving strategies or plans produced on behalf of the BCM Board.
- Achieving the BCM Objectives of the Force.
- Producing and maintaining auditable evidence of the implementation and maintenance of the BCM Programme.
- Monitoring and responding to changes in statutory requirements, indicated minimum standards set by authoritative bodies and identified good practice. This includes monitoring of implementation of this policy.
- The Chair of the Force Resilience Forum is the Assistant Chief Constable (Protective Services) or other person appointed by them.
- The guidance in the following documents will be taken into account when deciding the scope of BCM arrangements and acceptable minimum standards to be achieved.
- Cabinet Office – Expectations and Indicators of Good Practice – The Civil Contingencies Act 2004, its associated Regulations (2005) and Guidance, and the Resilience Capabilities Programme.
- ISO 22301 Business Continuity
- Home Office – Strategic Policing Requirement (July 2012).

2.7.   The aim should be to at least meet and preferably exceed the standards and requirements.

2.8.   The Chair of the Force Resilience Forum will be responsible for allocating responsibilities for the management of specific tasks or areas of work related to BCM to individuals as appropriate.

2.9.   Allocation should take into account the nature, scale, complexity, geographic location and criticality of business activities alongside Force culture, dependencies and operating environment. Division of responsibility along Departmental or Business Unit boundaries may not always be appropriate due to the complexity and interdependence of the organisation. There are very few areas of the force that undertake critical activities that can be delivered independently. It will therefore be necessary to establish processes that enable effective Business Continuity Management of all Critical Activities but avoid unnecessary duplication of effort or conflict.

2.10.   Where necessary persons representing organisations undertaking critical activities on behalf of the force may be required to participate in Force business continuity management processes and/or take responsibility for specific tasks or areas of work relating to business continuity management.

2.11.   The BCM Team within Operations, Integrated Emergency Management in line with the Force Resilience Forum will implement a rolling program of work in line with the Business Continuity Lifecycle detailed in ISO 22301. The program of work will aim to ensure all aspects of Force Activity are reviewed within a 5 year cycle. The Force Resilience Forum will decide the priority and timescales for this activity.

2.12.   The arrangements ensuring Critical Activities are maintained at or above acceptable minimum standards within the agreed maximum tolerable period of disruption for each activity will be based upon evidenced risk assessment.

2.13.   Strategies and Plans produced as a result of this policy will use Template Designs approved by the Force Resilience Forum.

2.14.   The Force Resilience Forum will be provided with access to appropriately skilled staff to support the implementation and maintenance of this BCM Policy.

Implications of the Policy

2.15.   It is recognised that the guidance contained under this heading may not be directly applicable to all policies. Where it is relevant however, the following areas should be considered:

Financial Implications/Best Value

2.16.   The Force Resilience Forum will be formed from currently serving employees including representative Chief Officers, Departmental Heads and Business Unit managers. These members of staff already complete some work related to Business Continuity Management. This policy will require them to do the same work within the framework set by the Policy.

2.17.　　It is expected that a significant amount of work is involved in implementing this policy. Business Impact Assessment and the production of Business Continuity Plans is time consuming and require staff with relevant expertise to complete the work. The Force has a dedicated team of trained business continuity professionals to manage completion of this work. Work may be achieved by the appointment of additional staff for this purpose or by the re-deployment or re-tasking of current staff.

2.18.　　Where requirements to undertake BCM related workload are included in commercial contracts it is expected this will be reflected in charges levied for service delivery. Such costs will be assessed and accepted as part of commercial negotiations at the time of contract development and management. In some cases it may be appropriate for contracted providers of goods or services to be represented at the FRF to allow the Forum to manage on-going costs and expectations.

2.19.　　The Force Resilience Forum will be responsible for making decisions about which of these methods is most appropriate and for producing a Business Case for any additional resources required.

2.20.　　It is expected compliance with this policy will be viewed as an enhancement to Best Value arrangements. Effective implementation will lead to more efficient use of the workforce and other resources.

Human Resources/Training

2.21.　　Members of the Force Resilience Forum may require training to ensure they are familiar with this Policy, the BCM Management Process and relevant indicators of good practice. It is anticipated this training can be delivered using current force resources, mainly by the Business Continuity Management Team.

2.22.　　The person or persons required to undertake the work of implementing and maintaining the BCM Policy and producing BC Plans should have the skills and knowledge relevant to 'NOS - CC AD1 - Develop, maintain and evaluate business continuity plans and arrangements' (Appendix C). This will be achieved by ensuring the Business Continuity Management Team has the skills and knowledge required, where necessary providing them with appropriate training. Training will generally involve attendance on a series of courses provided by recognised external training providers such as the Emergency Planning College, Business Continuity Institute or other accredited training providers. In total approximately 12 days training spread over 4 weeks combined with relevant experience will be required. It may take up to a year to complete such training and induction. Alternatively it may be felt appropriate to recruit a person or persons with the relevant skills into the force.

2.23.　　Persons required to maintain BC Plans should have received appropriate training. It is expected this would be provided by the Force Business Continuity Manager.

2.24.   Persons with key roles within any BC Plans produced will require initial training regarding their role within the plan followed by regular updates / exercises to refresh knowledge. It will be necessary for each BC Plan to contain an element setting out the training and exercise requirements. It is expected this training will be provided by a Department / Business Unit Head or the person who has written a specific plan.

Strategic/Business Plan

2.25.   Risks associated with the achievement of the Policing Plan and individual departmental plans are managed as part of the process.

Risk Management

2.26.   The Force Resilience Forum will be responsible for identifying risks to the BCM Process and either managing these or referring them to alternative risk management processes for management in accordance with the Organisational Risk Management Policy.

2.27.   The key risks to the implementation and continued compliance with the policy are:-

• Failure to ensure ownership of the policy at 'executive' level.
• Failure to appoint appropriately skilled persons with sufficient authority to membership of the Force Resilience Forum.
• Failure to appoint appropriately skilled person(s) who have adequate time and resources available to manage the day to day implementation and maintenance of the BCM Policy and production and maintenance of BC Plans
• Failure to include compliance with the BC Policy within the appraisal, reward and recognition processes used within the Force.

3.   UNDERPINNING POLICIES AND PROCEDURES

3.1.   To support the overarching WMP Business Continuity Policy the following policies will be maintained by the force –

1.   Physical security policy;
2.   Force Information Security Policy;
3.   Information Security Incident Management Policy;
4.   Information Services Risk Register;
5.   West Midlands Police Risk Appetite Statement;

4. EQUALITY IMPACT ASSESSMENT (EQIA).

4.1. The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how West Midlands Police has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

5. HUMAN RIGHTS.

5.1. This policy has been implemented and reviewed in accordance with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of West Midlands Police (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

6. FREEDOM OF INFORMATION (FOI).

6.1. Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.1 of this policy has been GPMS marked as Not Protectively Marked.

6.2. Public disclosure does not automatically apply to supporting force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number
N/A		

7. TRAINING.

7.1. There is no specific training for West Midlands Police personnel; however those individuals with a specific involvement in Business Continuity and Risk Management will have the relevant training courses detailed within their job specifications.

8. PROMOTION / DISTRIBUTION & MARKETING.

8.1. The following methods will be adopted to ensure full knowledge of the Policy:

- Newsbeat
- Intranet
- Posters
- Policy Portal

8.2. No uncontrolled printed versions of this document are to be made without the authorisation of the document owner.

9. REVIEW.

9.1. The policy business owner – Head of Information Management – maintains outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

9.2. The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

9.3. A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted annually as indicated on the first page.

9.4. Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

9.5. Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.

CHIEF CONSTABLE

10. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	24 December 2014	Initial Draft	Tom King/Stephen Laishley
0.2	14 January 2015	Amended Version	Kate Hitchcox/Stephen Laishley
0.2	10/02/2015	Policy approved by CC – policy reference, CC signature added.	56408 Couchman