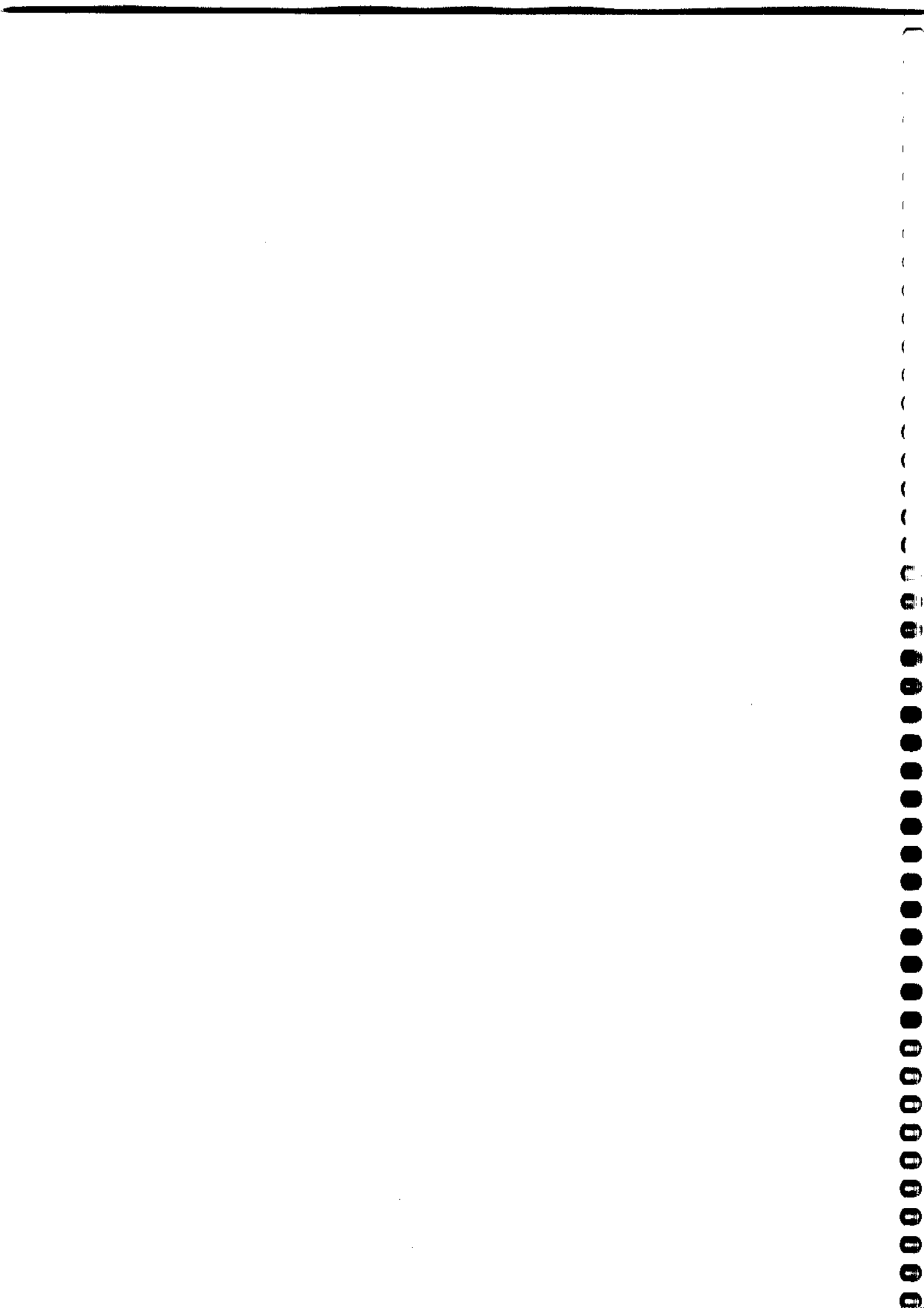


GREATER MANCHESTER POLICE

I.T. STRATEGY

2005 - 2009

Jen Mulcahy
Force I.T. Director



Executive Summary

The IT Strategy explains what we need to do with our Information and Communications Technology in order to help to make Greater Manchester safer. It provides the strategic direction for IT and a plan for the next five years. The Strategy will be formally reviewed every year and re-published if required. It will definitely be published every two years.

Section three describes the existing state of IT within GMP and relevant internal and external issues. The main external issues which affect our plans are: the five key priorities in the National Policing Plan, 2005-2008, the technology targets in the Police Science and Technology Strategy, 2004-2009; the proposed National Police Improvement Agency; The doctrine programme from Centrex, the findings from the Bichard enquiry in relation to the provision of a national nominal index and a national intelligence system; the Information Systems Strategy for the Police Service (ISS4PS); and the introduction of the Government Protective Marking Scheme.. Internally, the issues which affect our plans can be split into three categories: Business Systems; Infrastructure, and Service Delivery. From a business system perspective there are four main issues: Information Management; Partnerships; Call Handling and Contact Management; and Management Information. From an infrastructure perspective, the most significant are: Mobile Data; Infrastructure consolidation; Service Continuity and the revised environments for OPUS and Oracle Development. From a Service Delivery perspective they are: Performance Monitoring; Proactive management of the environment; and the introduction of Service Management.

Section four sets out a governance framework which details the policies and procedures that we will adopt to filter proposals and ensure successful implementations.

The policies are split into four separate categories: Management; Procurement; Project Management; and Technical Policies.

- The Management policies are designed to ensure that our I.T. Systems are consistent across the force. This will enable the Force to undertake comparative analysis, identify best practice and establish common standards.
- The Procurement policies are intended to ensure that the Force purchases applications that are appropriate, effective and efficient, and thus provide best value.
- The Project Management policies provide guidelines for implementing I.T. Projects.
- The Technical Policies are now contained within the Technical Architecture which has been expanded to include the principles by which we will manage and operate technology. These principles are designed to allow applications to reside on the same network without interfering with each other's activities. They also define a set of standards that allow applications to communicate and pass information between themselves.

All the policies must be followed whenever possible and contravened only where there is considerable justification and a full knowledge of the consequences. Systems which meet the user requirements but not the Force's IT standards are not considered acceptable.

The IT Procedures identify how proposals for new IT Systems can be put forward, how these proposals will be assessed; who is responsible for each aspect of the IT Strategy and how decisions are made. It outlines the role of COPG, ISSG and the IT Branch in relation to the IT Strategy.

It is unlikely that the governance framework will change much over the life of the strategy as consistent decision making is a requirement for successful delivery.

The IT Strategy programme (Section 5) sets out the schedule of developments and their relationship with corporate priorities.

- To reduce crime with our partners and communities
There are four pieces of work including the introduction of a computerised Case Handling system and sharing of information with other forces.
- To investigate and detect crime
There are nine pieces of work including a Crime Investigation system and a Force intelligence system.
- To provide reassurance to our communities
There are eight pieces of work including a Duty Management system and a Time and Attendance system.
- To ensure our organisation is effective and efficient and makes the best possible use of our resources
There are 20 pieces of work including a Document Management System and a Call Handling project.

In addition to the above there are 27 pieces of work in relation to the IT Infrastructure. These include: Replacement programmes for hardware and software; Digital recording, resilience in our connections to GPRS and the Internet; and Network time synchronisation.

The IT Strategy programme will be formally reviewed every six months and is likely to change more regularly than the rest of the document¹. Predicted timescales and costs for all work in the programme can be found at Appendix A.

The Technical Architecture for GMP is at Appendix B. This document will be revised and reissued during the life of the strategy and if you are unsure whether you have the correct version please contact the Programme Support Office

¹ If in doubt as to whether you have the most up to date version please contact the Programme Support Office ☎ 61355

1. INTRODUCTION

1.1 Why have an I.T. Strategy?

The IT Strategy exists to ensure strategic alignment of the business and its IT. The IT Strategy sets out the direction for IT, describes the projects we will deliver and explains the process by which changes can be made. In particular the Strategy provides:

- a strategic direction that aligns the Force and its IT to enable it to achieve outcomes such as: delivery of the National Intelligence Model; optimised performance; improved service delivery; flexibility to cope with change; and value for money.
- Identification of the strategic issues facing us - an agenda for change
- a governance framework for integrated decision taking.
- policies and standards for consistent approaches to the management of IT
- an IT architecture that supports business objectives
- A clear IT Strategy Programme and high level plans to realise that deployment

1.2 Structure of this document

The rest of this document sets out the strategic direction for our IT; the issues we currently face; the governance arrangements and the resultant IT Strategy Programme.

Section 2: Strategic Direction

Sets out the strategic direction which we should take in relation to our IT to optimise the delivery of our corporate priority.

Section 3: Strategic Issues

Describes the internal and external issues that affect the Force and prompt us to consider new IT systems.

Section 4: Governance Framework

Sets out the policies and procedures that we will adopt to filter proposals and ensure successful implementations and identifies who is responsible for each aspect of the IT Strategy and how decisions are made.

Section 5: IT Strategy programme

Links all the proposals for IT systems to our current priorities and targets.

Section 6: Monitoring progress

Identifies how we monitor our progress towards the implementation of the IT Strategy.

Appendix A: High Level Plans

A series of charts showing a schedule of the sequence of I.T. developments over the next five years and the corresponding Capital and Revenue expenditure programme.

Appendix B: GMP Technical Architecture

A detailed picture of GMP's Current, Interim and Strategic Technical Standards.

2. STRATEGIC DIRECTION

This section sets out the strategic priority for Greater Manchester Police and the strategic direction which we should take in relation to our IT to optimise the delivery of our priorities.

2.1 Strategic Priority

We are here to make Greater Manchester safer.

Our Strategic Aims are:

- Reduce crime and disorder within Greater Manchester with our partners and communities.
- Investigate and detect crime.
- Build safer communities with our partners.
- Provide a well led and accountable service that is efficient and effective.

2.2 Strategic Direction for IT

The Strategic direction for IT is to support these four key aims by providing all staff with the information they need to:

- Support and develop strategies and tactical plans
- Identify areas of enquiry through exception and trends
- Establish root causes and common characteristics
- Plan resources
- Deploy resources to match priorities and demands
- Set Targets
- Monitor performance
- Identify strengths and weaknesses
- Deliver accountability and value for money

3. STRATEGIC ISSUES

This section outlines the relevant issues which affect strategic IT planning and the existing state of IT within Greater Manchester Police.

3.1 External Issues

- The National Policing Plan 2005-2008 sets out the Home Secretary's five key priorities. We have made significant progress in some areas, notably in relation to the technology supporting the National Intelligence Model (NIM), Partnership working and the Prolific and other priority offenders strategy. This strategy will extend our work in these areas to cover the requirements of NIM2, the increase in partnership working, and the Professionalising Investigation Programme. Additionally, we will deliver ANPR to support the priorities of: Reducing Crime and Reducing concerns about crime, and support the achievement of the Citizen Focus priority by delivering technology to reduce bureaucracy and increase accessibility and contact. We will also support the achievement of the priority to Combat Serious and Organised Crime within and across force boundaries by delivering technology to support the set up of the Force's Counter Terrorist Unit.
- The Police Science & Technology Strategy 2004 – 2009 supports the National Policing Plan and contains specific targets for the delivery of certain technology. We have completed our Airwave roll out; implemented the national Violent and sex offenders register (ViSOR); met the target for all criminal justice professionals to have the capability to e-mail each other securely; and intend to implement NMIS by October, 2005. We will meet the target for the core criminal justice organisations to have electronic access to shared case file information by March 2006 by implementing NSPIS Case Preparation. We are expecting PITO to deliver the firearms registration (NFLMS) system during the next two years;
- the proposed creation of the National Police Improvement Agency and the setting up (in the interim) of the National Centre for Policing Excellence (NCPE) refer to co-operation between forces in general and the sharing of back office systems in particular. Sir Peter Gershon's, Independent Review of Public Sector Efficiency, published in 2004, sets targets for efficiency which may require technology to realise whilst at the same time changing the method by which it is procured and delivered. Both sets of changes could have significant impact on both IT infrastructure and forces' information systems
- The Doctrine programme will deliver guidance and best practice across a wide range of police business processes which may require the provision of new or amended systems.
- The Bichard Enquiry has highlighted the need to have common systems and processes for recording, analysing and disclosing intelligence and for sharing intelligence and other data items across forces. A proposed statutory code on the management of police information has been produced by ACPO and guidance on its implementation is expected in May, 2005. We intend to implement this code as part of a broader review of our approach to Information Management.
- In response to the Bichard Enquiry, PITO are promoting the development of Programme Impact. This will involve the development of a new centralised national intelligence system to handle intelligence reports and standard analysis tools and reports for all forces. We have already met our requirements to support the national nominal index (PLX) required by the Criminal Records Bureau (CRB) and we are required to share information from six systems (Crime, Intelligence,

Custody, Child Protection, Domestic Violence & Firearms) in Corporate Data Model format via a CRISP database by April 2006. We expect to receive a release of the CRISP Database in September, 2005. Programme Impact may require further amendment of our internal Intelligence systems and analysis tools.

- The National Strategy for Police Information Systems (NSPIS) has not provided the expected applications within a realistic timescale. Those that have been provided are proving expensive to implement and have significant revenue consequences. There may be no choice in the take up of some of the products. We have implemented three modules of NSPIS HR (Personnel Records, Training Administration, and Health and Safety) and are preparing to implement Duty Management (and a non-NSPIS Time and Attendance system to support collection of the data). We will implement NMIS during 2005 and plan to implement Case Preparation by 2006.
- In 2000 ACPD endorsed an Information Systems Strategy for the police service (ISS4PS), which was based upon a common infrastructure, central co-ordination of developments and common standards for the processing of data. Although the standards have not yet been defined and the strategy is currently under review, we do need to comply with the general principles of the ISS4PS.
- The introduction of the Government Protective Marking Scheme by the end of 2005 requires that all documents be protectively marked.
- The replacement for PNN2 – PNN3 - is currently out to tender.
- The replacement for VP/FPO is currently out to tender.

3.2 Internal Issues - I.T. Business Systems

Progress has been made on the issues outstanding at the time of the last strategy, we have continued to develop OPUS as single mechanism to provide all GMP staff and our partners with the information they need by including data from more systems, an interface to PNC, and photographs. We have significantly extended the functionality of OPUS through delivery of Forensic Action Management, Missing Persons, Family Support Investigation, Stop Search, SARA, POMAN, Action Management and a forcewide OPU. We have established a Data Management Team, replaced the ageing mainframe hardware systems for Personnel, Discipline & Complaints and Statistics; addressed the lack of strategic IT provision for Transport; and upgraded our analysis tools (i2). We have enhanced GMPICS to support the restructure of the force; the implementation of the National Crime recording standard; the national standard for Incident Recording; and the recording of Business Crime. We have delivered Lotus Notes systems in many areas as part of Approach replacement and also to support areas as diverse as Gold, Silver, Bronze support (GSB) Performance management (PAM). The main issues facing us at the time of this review are:

- **Information Management**

The requirements of the Bichard report, the proposed statutory code of practice on the Management of Police Information, the Doctrine programme, and the revised National Intelligence model (NIM2) can only be achieved if we manage our information as a corporate resource. Initial analysis of our corporate information in preparation for the introduction of our new Force Intelligence and Crime Investigation Systems indicates that we need to review our approach to the collection, processing and distribution of information. The Force has yet to

determine where overall responsibility for Information Management should reside, but the known implications for the IT Strategy at this stage are as follows.

We have previously agreed that the development of local systems by non IT staff must cease and existing local systems are being dealt with as part of an overall migration plan which continues to replace local systems with corporate ones. We will accelerate this programme by removing Lotus Approach from the desktop as part of the review of our PC standard.

We need to take a strategic view on the storage, transport and accessibility of photos, images, video clips and CCTV and then include access to them through the repository. We will do some research on facial recognition to support this.

We are committed to the nationally recommended Mapping Product, Blue8. We now have a strategic approach to geocoding, maps, and streets and premises but we need to integrate mapping more fully into OPUS as a standard mechanism for how we present information.

We need to take a strategic approach to how we manage records and documents and provide a system to support our obligations under the Freedom of Information Act and a forcewide electronic document records management system.

- **Partnerships**

One of the five key priorities in the National Policing Plan is that we should take action with partners to increase sanction detection rates and target prolific and other priority offenders. We have delivered the GMAC and POMAN systems and set up a partnership project. We need to replace our existing system for obtaining Prisoner Release information. The introduction of neighbourhood policing will increase the demand for local partnerships and the requirement to tackle level 2 criminality will increase the demand for sharing information across force boundaries. Local initiatives will also increase as more local control of spending is achieved through the force's devolution project, the continuation of the Basic Command Unit Fund in 2005/06, and the Safer and Stronger Communities fund becoming fully operational in 2006/07. The delivery of these initiatives may also require us to develop different mechanisms to safely share our information.

- **Call Handling and Contact Management**

One of the five key priorities in the National Policing Plan (greater detail in the 2004 Building Communities, Beating Crime report) is that we should provide a citizen focused police service. There is a stated intention to have a Single non-emergency number and a National Call Handling Strategy with Quality of Service targets. Call Handling is also a key objective for GMPA. We will scope our Call Handling and Contact Management project and start to deliver technology support where possible in 2005. As part of this scoping exercise we will take into account the national priorities and the recommendations from the force's 2004 Best Value review of Call Handling, the findings from Step Change, the HMIC report Open all Hours and their thematic inspection on Contact Management due during 2005.

- **Management Information**

We introduced the GRIPS system in 2004 to deliver consistent performance data down to individual officer level. The delivery of GRIPS and the Force's focus on performance have enabled the performance framework within GMP to evolve and mature. The GRIPS system no longer meets our needs and a situation has evolved whereby significant divisional resources are being used bridge the gap

with a consequential lack of consistency in our approach. We need to establish GRIPS as the recognised single source of data for Management Information. To do this we need to: upgrade the underlying technology (Business Objects); add the additional OPUS data from systems developed since GRIPS was launched, including the data from the Notes based PAM System; introduce the real time update of data into the OPUS environment (which will make it available for GRIPS) and provide the ability to drill down into the data.

- **Existing Systems needing investment**
- **GMPICS** - We will replace the Intelligence and Crime Investigation elements of GMPICS during 2005. We will review the Command and Control and Crime Recording elements during 2007/8. In the interim we will integrate the ICCS into our network, deliver AVLS and a more integrated presentation of resources on maps using dual screens, and upgrade the storage to allow for on-line FWIN retention for seven years.
- **Central Ticket Office** - The technology used to support the Central Ticket Office is currently independent of the IT Services Branch. It is not connected to our network or supported by our staff. During 2005, we will upgrade the existing application and infrastructure, provide scanning facilities, connect them to our network and establish our approach to the new national application (Pentip).
- **HOLMES II** - The technology on which our existing HOLMES system is provided will cease to be supported during 2006. We need to upgrade to a supported platform, integrate it into our Business Continuity provision and deliver the regional Casualty Bureau.
- **Discipline & Complaints** - The setting up of the Independent Police Complaints Commission has changed the way we handle complaints. We replaced our legacy system during 2004 and may be required to take the new national system in 2008. At the same time we will consider implementing a complementary system to support Civil Litigation.
- **Financial Systems** - During 2006 we need to look at taking support for the Contract Management System into the IT Services Branch and review the implications of any plans to implement the Euro. We will also consider upgrading our Car Loans and Payroll systems and all our financial hardware to support the next version of Oracle.
- **Other systems** - We need to enhance the encryption provided on PIMS, provide an Autoquote system and scope a project to deliver technology to manage Fraud Investigation. We will move to the National Special Branch system during 2006.

3.3 Internal Issues - I.T. Infrastructure

We have delivered increased reliability and performance in our infrastructure. Our main focus now is on ensuring that we provide continuity of service through increased resilience for our critical systems and the take on of services at the newly provided Business Continuity Site. The main issues now facing us are

- **Voice and Data Network**
We have delivered IP Telephony, replaced the Switchboard and integrated our voice and data networks into one common infrastructure. The new network has

an expected life beyond the life of this strategy. There have been some significant changes as our Estate has changed in line with the PFI project and this will continue in 2005. We need to complete our resilience testing of the new infrastructure, implement digital recording of all voice calls, make provision for the transmission of confidential information, and enable connection over broadband via VPN Tunnelling. Additionally, we need to increase the resilience of the core of the network as part of the move to service continuity and increase the capacity at the core to reflect the additional connections needed to provide resilience and remote monitoring for our centralised server population. As part of this work we will rationalise our accommodation to ensure that we only have two computer rooms. During 2005 we will deliver resilience and load balancing on GMP's internet connection and resilience for GPRS.

- **Cabling**

The introduction of IP Telephony and the integration of the previously separate voice and data services has provided standard cabling for voice and data in all our buildings.

- **Radios**

We completed the forcewide rollout of Airwave in October 2003. Our integration into the national Radio Scheme, providing effective network sharing for us to use other forces' infrastructure and for other forces to use ours, was effected by the upgrade to V5.1 in December, 2004. We have delivered outgoing telephony from Airwave but have no plans to allow members of the public to contact these numbers directly. The provision of Airwave for the Air Support Unit is still a temporary national solution and we will need to upgrade as soon as suitable equipment is available and has been certified. We still have some of our analogue radio infrastructure in order to support the need for Mutual Aid and the Home Office requirement to provide and monitor a designated VHF Calling Channel for visiting police forces and other designated agencies. The national roll out of Airwave is due to complete during 2005 and we will decommission the remaining analogue infrastructure during 2005. Additionally, we provide separate Cougar digital radios for some Force specialist Units. Cougar will be retained until Airwave can offer this service; this is unlikely to be prior to 2007.

- **Mobile Data**

We have delivered the mobile provision of personal data (Mail and Calendar) via GPRS Laptops and Blackberry handhelds, but have not yet started our Mobile Data pilot. The provision of significant national funds to support ANPR during 2005 will enable us to deliver an infrastructure to support mobile information in vehicles. We will use this infrastructure as part of our Mobile Data pilot with ANPR as the first application. We will also ensure provision of Laptops for all operational Superintendents to facilitate their ability to deliver 24x7. We intend to deliver Socrates information to mobile Crime Scene Examiners during 2006.

- **Access to PCs**

We now have over 5,500 PC's which is greater than the previous target of 5,000 and reflects the increase in establishment. There is still a view that there is insufficient provision for operational officers. We will review distribution when the support tools are in place to provide accurate information.

- **Infrastructure consolidation**

The server consolidation project, replacing the existing hundreds of distributed servers with fewer, larger, centralised servers is ongoing. We have consolidated

all personal data and shared areas and will complete the consolidation of mail files during 2005. We need to continue our progress towards Service Continuity by introducing clustering for our critical systems. In the first instance we will apply this to email, OPUS, Holmes and Duty Management. The implementation of Network Attached Storage complements the consolidation programme by allowing us to implement more effective capacity management and revised back-up and recovery arrangements in line with the service continuity requirements. We will also do some research on a 'Virtual Server' environment.

- **Development Environment**

During 2005 and 2006 we will develop and implement a new Crime Investigation System and a new Force Intelligence System. We need to ensure that the environment in which we intend to deliver these systems is upgraded to meet the availability and resilience targets which these critical systems require. During 2005 we will upgrade our complete Oracle environment to version 10g together with the required hardware upgrades and monitoring tools. This will enable us to proactively manage the systems and deliver our service continuity obligations. We will also upgrade our Business Objects environment to V6 to meet the demands of GRIPS.

- **Standard Desktop and Server Operating System**

The Windows NT operating system will go end of life during 2005. We will migrate our servers to Windows 2003 and our desktops to Windows XP Pro during 2005. We use SCO's Unixware as the operating system for many of our central servers. This product has now gone end of life and we have chosen Windows 2003 as its replacement. In those few instances where this is not an available choice we will use the Solaris Operating system. We will seek to migrate all existing SCO Unixware servers to the revised standards during 2005.

- **Notes/Domino Environment**

The requirement for remote and peripatetic users of email is increasing and our existing provision is cumbersome and unreliable. During 2005 we will complete the roll out of V6 which will alleviate this problem. We will also upgrade our Intranet and Development environments to V6 during 2005. During 2006 we will look at how we can provide a single, unified presentation of all messages (email, voicemail, fax and text message) from email.

- **Video Conferencing**

We will review our policy on video conferencing during 2006.

- **PNN**

We have split our two PNN connections so that one is physically provided from the Business Continuity Site. We will provide complete resilience (and the ability for any PC to access PNC) as part of the PNC Strategic Solution project during 2005. Our existing connections for PNN will be upgraded to be capable of providing 34meg, (2 meg available) as part of the national upgrade for IMPACT.

- **Silver Control**

We will upgrade our provision for Silver Controls during 2005

- **Network Time Synchronisation**

We need to ensure that we have a single time source for all our systems. We will implement the infrastructure to support this during 2005 and commence

migration of our legacy applications. All new applications will have this mandated once the service is available as part of our infrastructure

3.4 Service Delivery

The Branch strives to meet the Force's IT and telecommunications equipment needs by delivering and supporting over 5,500 PC's, 800 laptops and 1400 printers via a high speed network that serves in excess of 120 locations. In addition, we are responsible for 6,000 office based telephones, over 1,000 Mobile phones; 440 Fax Machines and all the Airwave handsets. We currently deliver functionality across the policing business and are constantly updating this provision. The main issues facing us in relation to Service Delivery are:

- **Performance Monitoring**

We have implemented Performance Indicators across the Branch. We need to review these indicators in line with the revised demands of devolution and identify and remedy those areas where we have insufficient information to set performance targets and monitor performance. In the first instance we need to provide these indicators on an individual account basis.

- **Performance Management**

We have delivered the SMS environment and toolset. During the roll out of XP we will use SMS to create software packages to ensure that we have a standard desktop. No software will be loaded without a package. We are also using SMS for remote access to devices and intend to introduce its ability to create the inventory during 2005. During 2005, we will complete the introduction of OMS to proactively manage the Oracle environment, MOM for the physical server hardware and ILO for remote control of servers, OTM for the phones and NMS for the network.

- **Service Recovery**

The Customer Survey undertaken during 2004 shows continuing improvement in Customer Satisfaction. The National Benchmarking Exercise has identified areas where we can improve our service further and an action plan is in place.

- **Business Continuity**

During 2004, our purpose built Business Continuity Facilities were developed at Claytonbrook and handed over early in 2005. During 2005 we will commission the building in line with the Service Continuity demands of the organisation, as outlined in the earlier paragraph on Infrastructure Consolidation.

- **Security and Access**

We have implemented two-factor authentication for Remote users and will continue to undertake an annual penetration test as part of the ACPO Community Security Policy. We will implement data encryption for Laptops as part of the XP Rollout. During 2006 we will review our Firewall provision and undertake research into single sign on and anti-spam technologies.

- **Account Management**

The Account Management service continues to evolve and grow (we now have five) as our customers' expectations mature. A review during 2005 will look to consolidate this evolution and take account of changes demanded by devolution.

- **Unattended Operations**

We have completed our move to Unattended Operations at Chester House and the Computer Room is now a fully automated environment. The Business Continuity site will be fully automated and run as a 'lights out' site from inception.

- **Out of hours cover.**

The move to unattended operations and the continuing delivery of new operationally critical systems required a review of how we provide cover out of hours. Call Out is now initiated through the Force Duty Inspector. We have set up the role of IT Services Duty Manager and provided access for this person to a number of specialist teams. This enables us to provide 24x7 support for our Critical Systems. Enhancements in our proactive monitoring arrangements together with increased resilience in the infrastructure should reduce the incidence of call out. The provision of remote control tools for servers and broadband access from home will reduce the need for visits to site.

- **Service Management.**

We have implemented new ITIL Service Management standards in the areas of performance monitoring, capacity management and change control. During 2005 we will implement availability, release and configuration management.

4. GOVERNANCE FRAMEWORK

Ensuring that we have a consistent, objective and effective governance framework for initiating I.T. developments is the core of our I.T. Strategy. Adherence to sensible technical and management guidelines, and the adoption of a strict project selection and monitoring method will increase the probability of successful IT delivery.

Our procedures are designed to ensure that only I.T. developments that support the Force Strategy will be progressed. Responsibility for the Force's investment in I.T. lies with the Force Strategic Management Board (FSMB). To provide the detailed scrutiny required, the force has set up an Information Systems Steering Group (ISSG), consisting of the ACO Resources, the Force Finance, Personnel and Corporate Development Directors, two Operational Chief Superintendents, one Detective Chief Superintendent, one departmental Superintendent, and the Force I.T. Director. All proposals for IT are channelled through ISSG.

Accordingly, our governance framework consists of three different strands.

- The first strand defines policies that will help us to avoid common mistakes in IT. If set up correctly, these policies will automatically avoid many of the pitfalls of delivering IT systems. We do not expect to change these policies significantly, since consistency of approach is one of the keys to successful IT systems, but we will change them if we find that they do not produce the right outcomes.
- The second strand defines procedures which set out how the Force will identify, assess and apply priority to potential IT developments. If these procedures are correct they will provide consistent, objective and successful IT systems within a framework which is flexible enough to allow for changing Force priorities.
- The third strand identifies who is responsible for applying the policies and procedures

Applying the IT Policies (Section 4.1) to the proposals which arise from our IT Procedures (Section 4.2) results in the IT Strategy Programme (Section 5).

4.1 I.T. Policies

We need an objective and effective set of rules and guidelines to ensure that we make consistent and sensible choices between competing projects and to ensure that their implementation is successful.

The policies are not just IT technical policies. In fact policies about what we try to computerise, how we select the appropriate system and how we manage IT projects have a much greater impact on the success of IT projects than the choice of technology we use.

The following section therefore sets out four sets of quite specific policies:

1. Management Policies
2. Procurement Policies
3. Project Management Policies
4. Technical Policies

These policies will vary as technology changes and the Force capability develops, but should be followed whenever possible, and contravened only where there is considerable justification and a full knowledge of the consequences.

4.1.1 Management Policies

Management policies are designed to ensure that our I.T. systems are consistent across the Force. This will enable the Force to undertake comparative analysis, identify best practice and establish common standards.

- **Manage IT at the Force Level**
Information, systems and data will be managed and developed from an enterprise perspective and data will be treated as a shared corporate asset.
- **The same application will be used for the same function across the Force**
Shared solutions must be used where divisions or departments have similar needs. This is likely to mean compromise. Where systems overlap, removal of redundant systems will be planned and followed through with sufficient investment.
- **Business processes must be the same across areas**
Using a common application will only be successful if the processes that it automates are the same. There will inevitably be arguments that some Divisions and Departments have different circumstances that warrant different practices; these arguments will have to be overwhelming to be acknowledged.
- **Install unique applications only for specialised departments**
Unique applications will only be installed where unique functions are identified (e.g. Transport) this does not imply any waiver of the other force IT Policies.
- **Stick to the essentials**
It is tempting when considering a new computer system to ask for all the things that you would like. But the more you try to cover, the less the chance of success. It is better to install a system that does the basics well and then consider how it can be enhanced as a separate project.
- **Re-use Assets**
Existing systems and data that meet these Policies should be exploited in preference to introducing new ones. This will include the use of standard IT tools across the force. Such tools can be used in a number of applications and are often supplied with the application. To reduce training, we should try to adhere to a standard set of tools, (e.g. either MapInfo or Blue8, but not both) whilst retaining a commitment to trial new developments
- **Ensure information has a system owner**
All information must have a defined owner who is responsible for the quality of information and the control of access to it. The owner must have the authority to authorise changes to the system. Systems with no defined owner will not be changed until an owner has been appointed.
- **Ensure compliance with the ACPO Community Security Policy**
All systems must comply with the ACPO Community Security Policy.
- **Remove Investment from Legacy Systems**
Systems that are planned to be replaced will not receive investment, other than essential maintenance, legal or regulatory changes.

4.1.2 Procurement Policies

Procurement policies are intended to ensure that the Force purchases IT Services and products that are appropriate, effective and efficient.

- **Optimise Total Costs not just Project Costs**
IT Investments will optimise life time costs/benefits rather than simply project costs/benefits. Projects will only be allowed to proceed once their total costs (including 'into production' and ongoing operational costs) are known.
- **Tried & tested solutions**
Although the Force will continue to be innovative in those core areas where it should be at the cutting edge (e.g. Intelligence) it will give preference to Standard Packages rather than building its own. The uncertainty of software development and the problems of support usually far outweigh any shortcomings of standard packages. The Force will adapt its processes to fit the package rather than adapting the package to fit the process.
- **Discourage software development by non professional developers**
Where software development is undertaken, it should be done by the I.T. Branch or commissioned by the I.T. Branch from a reputable software house. Those who wish to develop software should provide their business expertise to the IT Branch. The benefits of a professional service, with properly negotiated rates for delivery, enhancement and maintenance, far outweigh enthusiastic improvisation. The ability for local development will be removed as part of the replacement desktop. Systems developed or purchased independently will only receive support if no other solution is available and there is an operational need. The cost will be charged to the budget holder, be one time only and provide no ongoing commitment to further support.
- **Install independent applications for discrete processes**
Generally, integrated software applications should be avoided in favour of specific applications for specific needs. Integrated applications are difficult to install, costly to amend and become impossible to maintain. Independent applications should be interfaced rather than integrated.
- **Trial new applications thoroughly**
All new applications should be trialed on a local basis, to a rigorous standard, before forcewide acceptance. The purpose of a trial is to evaluate the benefits to operational performance and the option to abandon a project should be actively considered, even at this late stage, if essential needs are not fulfilled.
- **Implement incrementally, rather than "big bang"**
Wherever possible, new applications should be implemented in small steps to facilitate effective management, minimise error, and enable swift rectification.
- **Prove system operability**
A system will only be deployed once it is proven to be sufficiently stable and operable to be supported to the required SLS's, and these SLS's will be defined so that the system is fit for purpose.
- **Enforce technical standards and policies**
All systems must conform to the Force's IT Technical Standards and Policies. Systems which meet the user requirements, but not the Force's IT standards should not be installed. Not only could such systems interfere with the operation of other systems, but the Force would be unable to link such systems together.
- **Use Long Term Strategic Relationships**
IT Services and products will be procured from established suppliers with whom the development of a long term strategic relationship is planned or underway.

This will be reflected in the contract arrangements which will clearly establish how our suppliers' performance will be monitored and managed

4.1.3 Project Management Policies

Project Management policies provide guidelines for implementing I.T. Projects. I.T. Projects are those projects in the programme managed by ISSG.

- **Concentrate on the processes rather than the IT**
Technology has the capacity to mesmerise users into seeing solutions before defining problems. It is essential that we review the processes that we intend to automate, before selecting any applications. In considering any process we must look at all the adjacent and related processes rather than just the element designated for automation.
- **Avoid inertia**
Although IT can enable change, it can also stifle progress. Once an application is installed the effort and cost in making changes often acts as a barrier to change. We should question existing applications and procedures, before considering new ones.
- **Divide IT projects into stages**
Costs, time scales and critical success factors cannot be realistically identified at the beginning of a project. A staged approach allows regular reviews and better informed decision making, which will eliminate disasters and cut losses.
- **Set clear objectives**
The biggest cause of project failure is unclear objectives. Without clear objectives the scope and range of the project can drift as people try to install what they think is required.
- **Allocate sufficient budget and resources to IT before the project begins**
People who propose an IT project must, in conjunction with the I.T. Branch, provide realistic estimates based on experience, not hope. Estimates should never be reduced to provide a business case. And then management should allocate sufficient time, money and resources to the project. If we are not prepared to do the job properly, we should not start it.
- **Consider Training Implications**
Any new system will only be effective if people understand how to use it. We must consider the training implications at the initiation of the project and make provision for them in the IT Training Strategy.
- **Follow Project Management Standards**
Detailed Project Management Standards (to PRINCE II equivalent) have been developed by the I.T. Branch. There are three groups of standards based on the complexity of the project and the risk of failure. These will be followed for all IT Projects and support in their use will be provided by the I.T. Branch's Programme Support Office.

4.1.4 Technical Policies

Technical policies are designed to allow applications to reside on the same network, without interfering with each other's activities. They also define a set of standards that allow applications to communicate and pass information between themselves. All of our technical policies and standards are contained within our Technical Architecture an extract of which is attached at Appendix B.

4.2 I.T. Procedures

The policies defined in the previous section are a set of rules that help us to avoid mistakes in implementing IT systems. However, before we can judge a system against these rules, we need to identify potential projects and decide to what extent they will meet our business objectives.

4.2.1 Identification of Potential Systems

Ideas for new computer systems come from many different sources, and we must be careful that our procedures don't inhibit any suggestions. The purpose of the identification phase is to get as many proposals as possible. They may be rejected later, but if they are never put forward, we will not have the chance to assess their worth.

Our procedures identify eight ways of putting forward proposals for using IT to improve the performance of the Force:

- **Force Strategy:** As part of the Corporate Strategy to develop the Force, processes and functions that would benefit from new computer systems will be identified.
- **Invitation to Bid for Funds:** Each year a capital bid process will allow any member of the Force to make a case for new or replacement IT systems.
- **The I.T. Branch** will put forward proposals for the maintenance of IT infrastructure (cabling, networks, security, and monitoring systems, etc).
- **Divisional and Departmental Budgets:** Divisional Commanders and Heads of Departments can use their own revenue budgets to purchase IT Systems.
- **Information Systems and Futures Group:** ISFG members can identify suitable systems for development and ways to increase the effectiveness of our existing IT Systems.
- **GMPICS Changes Group:** manages changes to improve our use of GMPICS.
- **PNC Steering Group:** manages changes to improve our use of PNC.
- **User Groups of National Systems**

In the support of this process, the I.T. Branch will ensure that the Force is aware of developments in technology or applications of existing technology elsewhere.

4.2.2 Assessment of Proposals

The only reason we would want to implement a new IT system is if we expect the new system to have a positive effect on the Force's operation. All proposals will be submitted to the Information Systems Steering Group, where the business and technology implications of the proposals are judged against three criteria:

- **Project Urgency:** Is the project Critical, Important or Desirable.
- **What Costs and Benefits** will the proposal deliver to the Force?
- **What risks** could affect the success of the project?

The I.T. Branch will also put forward its assessment of the technical complexity of the proposal and its odds of success. A poor technical assessment will not disqualify any proposal but will be weighed by the IT Steering Group against the cost of implementation and the potential benefits should the new system be a success.

4.2.3 Applying priority to competing proposals

The Force has limited funds and finite resources. Experience to date shows us that there are more potentially beneficial IT developments than we can accommodate. We therefore need to apply priorities to the list of beneficial proposals.

The first tranche of work will always include those systems that the IT Steering Group classifies as essential. Examples include replacement of redundant equipment, or directions from central government.

Beyond these essential systems though, each proposal will be given a score that reflects the net benefits of implementation (improved service, reduced costs, less risk) divided by the cost of implementation (time and money). Proposals with the highest score will be scheduled first.

By this method proposals with the best return are carried out first. Interestingly this method tends to favour small, quick projects over larger, longer projects.

Although the Information Systems Steering Group is given a financial limit as a guideline, its role is to present a prioritised, costed list to FSMB. The decision about how much to spend on IT developments in total (i.e. where to draw the line) rests with FSMB. If the benefits of new IT systems are great enough they can (and in the past, have) increased the force's expenditure on IT systems.

4.2.4 Implementation and Control of IT Projects

We only implement IT systems if we expect the new system to have a positive effect on the Force's operation. This may be improved business processes or compliance with legislation. Therefore the IT project must be part of a wider project, and that wider project should be under the control of the appropriate users.

On the other hand, IT is a specialised field and needs the technical expertise of dedicated IT staff. We will therefore appoint an IT person to be responsible for the IT aspects of each project and the I.T. Branch will maintain project control systems for each piece of IT work.

However, to ensure that the user maintains control over IT projects, each IT project will be divided into a number of designated stages. Monitoring the progress of each IT project and the decision to progress to the next stage will be the responsibility of the Project Board for the overall project. Key to these decisions will be the Project Sponsor (the Executive on the Project Board) who is responsible to the Force for the delivery of the benefits identified at the start of the project. To assist the Project Sponsor, each Project Board will have a Senior Manager from the I.T. Branch allocated as a member.

4.3. Roles & Responsibilities

There are three main bodies involved in the implementation, operation and review of the Force's IT Strategy

4.3.1 Force Strategic Management Board

The role of the Force Strategic Management Board within the Strategy is to:

- Sponsor the Force IT Strategy
- Ensure the IT Strategy maintains strong and consistent links with the Force Strategy
- Identify strategic issues
- Review the recommendations of the Information Systems Steering Group
- Authorise the allocation of resources

4.3.2 Information Systems Steering Group (ISSG)

The role of ISSG within the Force IT Strategy is to:

- Ensure that proposals put to the Force Strategic Management Board have clear business objectives and are properly costed
- Ensure that requests for IT developments are consistent with the Force IT Strategy
- Assess the impact of proposals on the Force's objectives and operating costs
- Filter and apply priority to proposals for IT projects
- Recommend a programme of IT developments to FSMB
- Review the progress of approved IT developments
- Monitor the programme and the financial implications of projects during the year and report variations appropriately.
- Decide if IT projects which have exceeded their agreed tolerances should progress to their next stage of implementation
- Recommend changes in IT Policy to FSMB

4.3.3 Information Technology Branch

The role of the Force Information Technology Branch within the IT Strategy is to:

- Deliver IT services to an agreed standard to enable the delivery of operational policing services to reduce crime
- Identify potentially useful new technology
- Enforce technical standards and procurement policies
- Ensure that proposals for IT developments are technically feasible
- Manage internal IT resources and external suppliers
- Deliver the Force's programme of IT developments
- Report upon progress in key strategic areas
- Ensure that User consultation is effective (Local User Groups, Force User Group)

5. IT STRATEGY PROGRAMME

This section lists the proposals for IT developments. Each proposal was assessed by the Information Systems Steering Group and then prioritised according to the procedures outlined in Section 4. The final schedule of developments, including financial implications is shown in Appendix A.

5.1 To Reduce Crime with our partners and communities.

Proposals

- 5.1.1 Implement a computerised Case Handling system.
- 5.1.2 Deliver sharing of information via Crisp
- 5.1.3 Provide a strategic and integrated approach to enable partnership working.
- 5.1.4 Upgrade to V2 of i2 Analysts workstation for tactical and strategic analysts.

5.2 To investigate and detect crime.

Proposals

- 5.2.1 Develop a system to support Crime Investigation.
- 5.2.2 Develop a forcewide Intelligence System.
- 5.2.3 Develop the OPUS repository.
- 5.2.4 Implement the national firearms licensing management system.
- 5.2.5 Deliver forcewide ANPR.
- 5.2.6 Provide a corporate image repository.
- 5.2.7 Provide a system to support Fraud Management.
- 5.2.8 Upgrade Holmes II.
- 5.2.9 Automate Prison Release updates.

5.3 To provide reassurance to our communities.

Proposals

- 5.3.1 Implement digital maps as part of GMPICS to provide better address referencing and quick identification of repeat victimisation - GIS-Digital Mapping.
- 5.3.2 Implement NSPIS Human Resources – Duty Management.
- 5.3.3 Implement a Time and Attendance System.
- 5.3.4 Implement a system to support the Freedom of Information Act.
- 5.3.5 Provide Networked CCTV.
- 5.3.6 Implement a Regional Casualty Bureau.
- 5.3.7 Undertake a mobile data pilot.
- 5.3.8 Prepare and set up for the Labour Party Conference.

5.4 To ensure that our organisation is effective and efficient and makes the best possible use of our resources.

Proposals

- 5.4.1 Provide forcewide management information in relation to our performance - NMIS.
- 5.4.2 Provide mobile facilities for Crime Scene Examiners.
- 5.4.3 Implement a system to record and track Property.
- 5.4.4 Upgrade the Payroll and Expenses systems.

- 5.4.5 Review and Upgrade the Estates systems.
- 5.4.6 Integrate the ICCS into the GMP infrastructure
- 5.4.7 Deliver a strategic approach to corporate image storage
- 5.4.8 Complete Airwave in-building coverage.
- 5.4.9 Upgrade Airwave ASU Provision.
- 5.4.10 Move Blackberries from pilot to production.
- 5.4.11 Deliver Document Management/EDRMS
- 5.4.12 Enable the transmission of confidential information across the network
- 5.4.13 Upgrade/Replace PIMS to deliver enhanced encryption
- 5.4.14 Provide mobile facilities for all operational Supts
- 5.4.15 Upgrade GMPICS to allow on-line FWIN retention for seven years.
- 5.4.16 Connect CTO to GMP network, upgrade the application and infrastructure and provide scanning facilities.
- 5.3.9 Research requirements of OCR's and start pilots of possible solutions.
- 5.3.10 Research and implement a single directory of names and access rights
- 5.4.19 Prepare for the introduction of the euro.
- 5.4.20 Provide Web Based access for GMPICS

5.5 I.T. Infrastructure.

Alongside the development areas we need to address the problems of the IT infrastructure; the underlying technology which is common to all our systems.

Proposals

- 5.5.1 Replace annually all PCs which are five years old.
- 5.5.2 Replace/upgrade annually all servers which are three years old.
- 5.5.3 Replace Scanners and Printers which are end of life.
- 5.5.4 Review the resilience of our PNN connections.
- 5.5.5 Implement tools which allow us to proactively manage the performance of our Oracle environment (OMS).
- 5.5.6 Review existing Disaster Recover provision, implement separate site and provide full Business Continuity plans.
- 5.5.7 Implement the infrastructure to support a single database (Oracle) and reporting tool (Business Objects).
- 5.5.8 Take a strategic approach to the provision of Silver Controls.
- 5.5.9 Adopt ITIL Standards
- 5.5.10 Undertake external tests of our IT Infrastructure.
- 5.5.11 Review our compliance with the ACPO CSP & the implications of MoPS.
- 5.5.12 Upgrade the Domino environment
- 5.5.13 Replace NT4
- 5.5.14 Replace local Approach systems
- 5.5.15 Provide digital recording.
- 5.5.16 Replace fax machines with Fax Senior.
- 5.5.17 Decommission Lotus Smartsuite
- 5.5.18 PNC Access Strategic Solution
- 5.5.19 Network time synchronisation
- 5.5.20 SMS Implementation
- 5.5.21 Upgrade our CJX Capacity
- 5.5.22 Core network expansion
- 5.5.23 Licensing costs
- 5.5.24 Data Integrity
- 5.5.25 Provide a resilient GPRS connection
- 5.5.26 Provide a resilient Internet connection
- 5.5.27 Allow use of Broadband by implementation of VPN tunnelling.

6. MONITORING PROGRESS

We will monitor delivery of the Strategy through ISSG.

6.1 Format of reporting

We will provide the latest monthly update on all projects in the IT Strategy Programme to each ISSG. For each project, this will provide a brief summary of progress since the last meeting and an indication of the overall health of the project (based on the Red, Amber, Green traffic light system). In addition it will show projects on-hold, projects not started and projects closed.

We will provide a set of performance indicators to each ISSG. This will show our performance against the delivery of operational service delivery targets e.g. Help desk calls; system availability; and service level statements.

6.2 Managing Performance

The reporting process is underpinned by the weekly IT Services Branch Senior Management Team review of performance. Each week a different aspect of our performance is considered so that over each month all aspects are considered. The current framework is reflected below:

Week One Work Programme (Infrastructure)	Capital Programme – Review of progress, changes, resourcing; Work Requests review of Progress, changes, resourcing; Changes to Technical Policies and Standards. Revenue.
Week Two Work Programme (Business Systems)	Capital Programme – Review of progress, changes, budget, resourcing; Work Requests (from ISFG, GMPICS Changes, Account Managers) review of Progress, changes, resourcing
Week Three Branch Planning	Budgets; Health and Safety; Accommodation; Training Plan; Staffing Matters
Week Four Branch Performance	Performance Indicators – Internal (Vacancies, Sickness, Appraisal, Fault fix performance, system availability, planned and unplanned downtime); and External (Computacenter, BT, Synstar, Vivista) Benchmarking; Internal Processes; Review of Contracts
Quarterly	IT Strategy; Branch Business Plan; and Branch Communication.

6.2 Regular Review

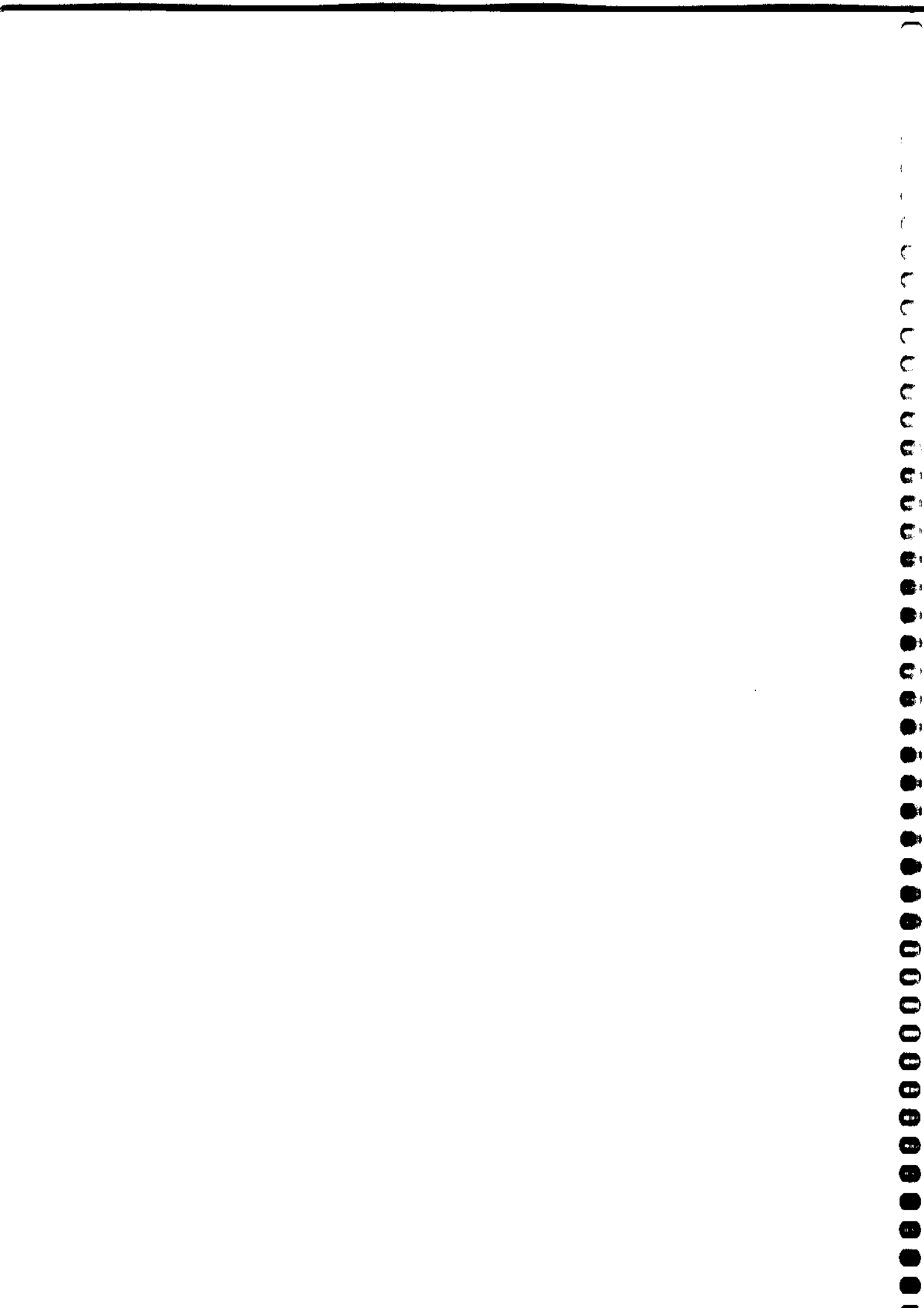
The IT Strategy is a working document, and it will be revised and amended as and when necessary to ensure that it remains linked to the Force objectives, takes advantage of technological development and directs activity to emerging strategic issues. It will be formally reviewed (and re-issued if necessary) every year and it will always be reissued every two years.

The Strategy will be formulated to take account of the demands of key users, stakeholders, and customers, and will cater for the limitations of and embrace developments within the IT industry.

7. REFERENCES

This section refers to the main documents which have influenced the IT Strategy.

- The National Policing Plan 2005-2008
- The National Intelligence Model Vesion2.
- The Police Science and Technology Strategy 2004-2009
- Sir Peter Gershon's Independent Review of Public Sector Efficiency, July 2004.
- The Bichard Inquiry Report, June 2004
- ACPO Proposed statutory code on the management of police information.
- NSPIS Standards and Plans.
- Building Communities, Beating Crime, 2004
- House of Commons, Home Affairs Committee, Police Reform, Fourth report of session, 2004-5, Vols 1 and 11.



Appendix A: PROGRAMME OF IT DEVELOPMENTS

Our programme of IT Developments is reviewed and updated at the start of each financial year. The latest programme available defined the five financial years beginning April 2005. The programme is subject to formal review every six months, and often changes as more accurate information on the scope and scale of our development is established.

It is important that any consideration of our developments is based on the most up to date version of the programme. For that reason the document is not included here. It is available from the Programme Support Office. In considering whether you need a copy of the plan please be advised that the plan is spread over a number of pages. For each project we show the estimated start and duration and the estimated capital and revenue consequences. We have no specific information on any projects (except those that are already in progress). The figures are 'ball park' estimates intended only to give an idea of the scale of costs and effort in the future.

The programme shows all bids, even those which did not make it into the current year's programme. This allows us to manage better any changes in circumstances (funding or resources) by stopping the least important or bringing forward the next most important bids.

It should be noted that projects not shown in the current financial year are not guaranteed to be progressed in the year in which they are shown or at all. That decision will be made on annual basis where they will take their chance with the new bids which have appeared in the interim period.



IT Services

TECHNICAL ARCHITECTURE 2005

Extract of Technical Policies

This appendix contains an extract of the technical policies from the Technical Architecture. The remaining sections of the Technical Architecture contain the detailed descriptions of the relevant environments and the current supported products at the time that this strategy was published. As such they are indicative of the level at which we manage our technology and are not included here.

1 Introduction

1.1 What is the Technical Architecture?

The Technical Architecture describes the information technology infrastructure that supports all applications used by GMP. The purpose of the architecture is to guide the development of the information technology infrastructure. The architecture establishes consistency by helping to:

- Provide managers and staff in the various IT units and support services with an understanding of the information systems infrastructure they are using
- Ensure that any products delivered into the GMP Infrastructure are fully compliant with it and do not modify or amend it.
- Provide a stable environment without impeding innovation and enabling the implementation of the IT Strategy.
- Provide standards for other IT organisations who need to communicate with GMP.

This Force-wide Technical Architecture currently describes:

- All of the information technology used and planned for use within GMP.
- The architectures of GMP applications (but not their application-related content).
- The standards and components that must be used in the development and delivery of information systems services within GMP.

1.2 Structure.

The Technical Architecture is divided into three core sections:

- **Architectural Principles:**
This section details the principles by which GMP manages and operates Information Technology.
- **Technical Environment:**
This section includes environmental descriptions for: Application Software, Data Management, Hardware, Network Architecture, Security Architecture and Radio Architecture.
- **Configuration Items:**
This section provides a comprehensive list of products and versions.

NOTE this extract only contains the Architectural Principles.

2. **Architectural Principles.**

2.1 **How we manage technology?**

• **Minimise complexity and Business Risk**

We will adopt recent proven technologies, from well established suppliers, which comply with our published Technical Architecture. Systems (applications, data and technology) will be designed as part of an overall architecture in order to reduce complexity and ensure business stability is not jeopardised.

• **Standard Products and automated distribution**

GMP will use the same standard products across the force and will use automated software distribution tools for their installation. All software will have a MSI package distributed via SMS. Upgrades to subsequent versions will also be done force-wide, automatically as part of a planned upgrade. Projects to implement new applications should not assume that they can use a different version of standard software or that it is easy to change the standard version.

• **Software applications must be hardware independent**

The purchase of software applications that run on only one manufacturer's hardware imposes commercial restrictions (monopoly supplier) and technical limitations (by restricting access from terminals) and should be avoided.

• **PC's should be application independent**

PC's should be capable of running any of the Force's software applications.

• **Applications must be independent of network addresses**

Software applications should not store the location and identity of the PC. If they do, PC's cannot be moved without reconfiguring of the application.

• **Centralised resources for processing, data storage and protection of systems**

Keeping systems separate reduces the risk of problems disrupting more than one system but can be cost inefficient in terms of wasted resources (processing, storage, licensing). We will share resources across systems according to Service Continuity categories. Shared resources will be designed to operate at the highest level of Service Continuity that is required from the systems running on them.

• **Manage the environment not individual pieces of equipment**

Because we share resources, changes to one system may affect the operation of others, which also share that resource. All changes will be implemented as part of the Change Management process and take account of our service level targets for all systems affected by the change. Access rights to make changes will only be available to a restricted group of people.

• **Service continuity not Business Continuity**

Critical systems will have sufficient resilience to ensure that they do not require downtime for routine upgrades or hardware failures. In the event of failure we will seek to return to the last known good state rather than trying to implement fixes in an ad-hoc manner.

• **Data Management**

Applications used in more than one part of the Force must share a single common data store, to ensure consistency of data, Force wide access and adequate backup and restore provision.

• **Shared applications must hold data in a single place**

We will hold our data in a single central place and back up and restore data in line with the service continuity definitions. We will take no responsibility for data stored

locally and will not attempt to restore or recover such data. We will standardise our data through Central tables of standard codes and aim to have: one central personnel system; one, central gazetteer; one central database for nominals; and one central database for vehicles. We will manage access to our data through one single user directory and a central directory service, which all applications, regardless of provenance will be required to use.

- **Audit logs**
All systems should maintain an inviolate audit log of user, location, date/time and data for all read, write and print activity. After a fixed period this information needs to be archived from the original application for longer-term storage and analysis.
- **Design for integration and flexibility**
Systems will be designed with a key aim of simplifying their integration with other systems including other forces and partners. Interfaces will use open or industry standards.
- **Interface standards**
ODBC allows us to transfer information between many different database formats. It should be the preferred method used for the transfers of information between police systems and especially for on-line transfers. XML, because it is self-documenting, is likely to be preferred for interfaces with external parties or when sharing information with more than one system as the data format is more easily reusable. If neither ODBC nor XML can be used then CSV should be considered. No proprietary interface solutions should be considered.
- **Local users must have access to and control of their own information**
Despite having a single data store, local units must have full control over their information, including creation, amendment and deletion of records.
- **All applications must use standard communications protocols**
In our case this is IP. This enables applications to 'speak the same language' and therefore communicate over the same network.
- **Standardise our operating systems**
To enable effective support, the Force will allow only a limited number of operating systems: Windows 2003 for servers and Windows XP for PCs.
- **Adopt national technical standards**
To enable our interaction with other forces, we will adopt national technical standards where possible. These will be reflected in our Technical Architecture
- **Use NSPIS applications**
The Force will, wherever practicable², select NSPIS approved applications.
- **Anticipate Mobile Information**
New applications must be designed to allow simple enquiries and data entry from a mobile terminal where appropriate.
- **Time synchronisation**
For business reasons it is essential that all force applications use the same time, to the nearest minute. We will make a resilient Time Synchronisation source available, which will be cascaded, to all servers and workstations on the network. Applications must always use server time as the definitive time for time stamping transactions. Applications should not attempt to synchronise PC times with server times.

² They meet the users' needs; they are commercially available; the requisite technical infrastructure to support them is in place; the systems they replace have reached the end of their useful life; the finance is available; and they are a priority in relation to the force's objectives.

- **Remote support by suppliers**
Access to the GMP network is tightly controlled by operational requirements and our obligations under the ACPO Community Security Policy. If remote support privileges are granted to suppliers then they will be subject to strictly defined non-negotiable criteria.
- **Access to Systems**
We apply security and access policies to all our systems and force regular password changes the use of hard coded passwords is unacceptable. We are aiming for a single directory and a single Portal that will control access to all our systems.
- **Escrow Agreements**
We will enter into Escrow agreements based on a risk assessment which considers the impact on the force were the application to be withdrawn and the likelihood of the supplier disappearing.

2.2 How we operate technology?

- **Computer room is Unattended and Access controlled**
The computer room is not manned. We will deploy automated systems and use software tools to monitor, record, detect and respond to system problems. Access to computer rooms will be strictly controlled and audited.
- **Servers will be centrally located, racked and controlled remotely**
As we run a "lights out" computer room, servers must be capable of being operated remotely from different offices or from home by on-call staff. Remote control facilities should include all keyboard, mouse, monitor and power supply recycling functions. No servers will be located outside the computer room. All servers will be in racks. We will not use pc's as servers.
- **We will remove single points of failure**
Servers will have at least two network connections to different network switches. The system will be able to operate normally on one set of connections. There will also be a third connection for the remote control. All Server racks will be on an independent, monitored UPS. Servers will have two power supplies, preferably hot swappable.
- **Performance will be automatically monitored**
All systems (network, servers, NAS, Printers, UPS) will be continuously monitored by specialist software for processor and memory utilisation, available disk capacity, rate of utilisation etc. Warnings, alerts and responses to problems will be fully automated. The specialist software will be standard across platforms and subject to the same controls as all other software.
- **Network termination cabling will be standard**
All cables will be labelled. They will be contained within network cabinets and these cabinets will be locked.
- **All Printing will be to network printers**
Printing must be capable of being controlled and monitored centrally. All printing must be capable of being directed to any printer on the network. The Printers we deploy will be standard with standard settings, which are locked down. It should not be assumed that different settings can be used or that it is easy to change the standard settings.
- **Types of systems for Business Continuity purposes**
Each business system within GMP has a different cost benefit justification for the investment required in business continuity or disaster recovery services. Whilst we

may prefer all systems to be fully resilient, this is not always necessary or cost effective. We will categorise systems according to the level of resilience we will provide in line with our Service Continuity Policy.

- **Fault Reporting**
A standard method of reporting faults is required. GMP has adopted ITIL standards for the management of incidents and would expect a similar process for reporting faults to external suppliers
- **Change Control**
GMP has adopted ITIL standards for change management and expects suppliers to have similar processes and to feed their Forward Schedule of Changes (FSC) into our Change Advisory Board (CAB). Changes to these technical standards will be dealt with in the same way.
- **We will not use system administrator or default rights**
It is poor practice for applications and system software to make use of default installation account names and passwords as these compromise the security of the application. Nor should applications make use of default privileged roles. GMP will delete these default roles and configure alternative provision.
- **We will have separate live and test systems**
New versions of software can be unreliable and have the potential to seriously disrupt the provision of service. All systems will make separate provision for testing of new versions. Changes to systems will not be applied directly to the live environment. The movement of changes from test into live will be governed by our Change Control Standards.