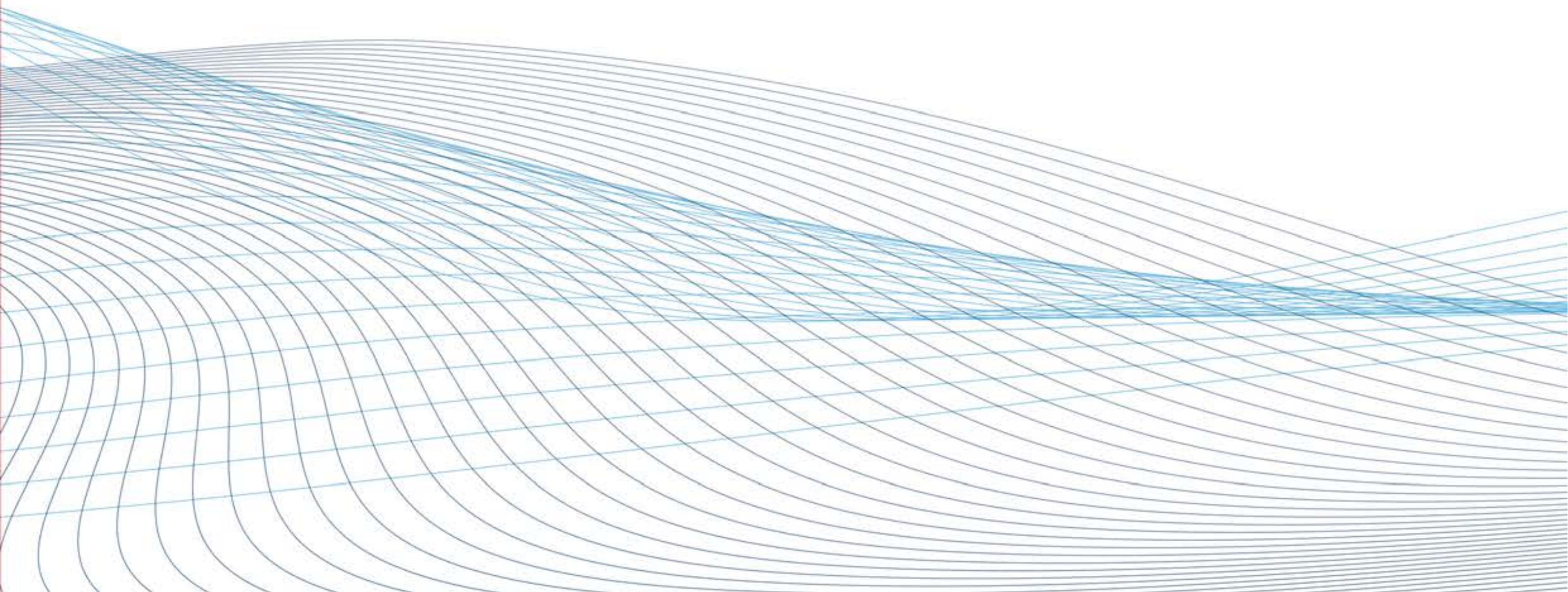
BACS APPROVED BUREAU SCHEME SUPPORT GUIDELINES

Security

VERSION 9.1 | May 2017



bacs

CONTENTS

1 DOCUMENT INFORMATION

1.1 VERSION HISTORY

VERSION	DATE	DESCRIPTION
9.1	May 2017	Rebranded and contacts updated

1.2 DOCUMENT REVIEWERS

STAKEHOLDER	ACTION		STAKEHOLDER	ACTION
BABS Team	P			
Operations Team	R			

Action: P – Producer; C – Contributor; R – Reviewer; A - Authoriser; I - Information only

1.3 COPYRIGHT STATEMENT

2 INTRODUCTION

These guidelines have been produced for use by organisations that run computer systems that prepare and submit financial transactions for automated payment, or collection, to VocaLink Limited for processing through the Bacs clearing system. The guidelines aim to provide an indication of those areas where security controls and procedures should be in place in order to reduce and limit the potential risk of damage to organisations' Bacs processes and Bacs related data, including any processes relating to the Faster Payments Direct Corporate Access (DCA) Service.

Unless stated otherwise, references to the Bacs service throughout this document also apply to the Faster Payments DCA service.

Damage may be incurred deliberately or accidentally. It is unlikely that any organisation can reduce risk of damage to zero. However, the implementation of appropriate security controls and procedures can reduce risk levels and detect and limit any damage caused. They can also provide and enable data and system recovery in order to maintain business continuity and the reputation and credibility of the organisation.

The Bacs clearing enables payments and collections to be made in a convenient and cost effective manner. Its use, however, has to be balanced, assessed and managed against the risk and cost of appropriate security controls and procedures required to protect them.

Risk assessment and management must be practical and appropriate to the size and complexity of an organisation. It should take into account the potential consequences resulting from damage to the organisation whilst being realistic as to the probability of it occurring. Controls and procedures introduced should be justified according to the risk assessment.

The security control procedures and recommendations described in these guidelines should be interpreted within the context of those currently existing within an organisation. We recommend, however, that if there are areas of potential risk identified from the use of these guidelines, those areas should be examined and the appropriate controls introduced. Procedures should be introduced and formalized in a documented manner.

3 BACS PAYMENT SCHEMES LIMITED

Bacs Payment Schemes Limited (www.bacs.co.uk) is the membership based, not for profit industry body whose role is to develop, enhance and promote the use and integrity of automated payment and payment related services. It also governs the rules and legal structures under which payments are made and promotes best practice amongst those companies who offer payment services. Its principal products are Direct Debit and Direct Credit, which are also used to effect standing orders.

3.1 THE MEMBERS

The Bacs website (www.bacs.co.uk) provides details of all Bacs Members.

The "Members" act as sponsors for existing users and bureaux as well as for organisations who may wish to become service users. Should an organisation wish to submit transactions on behalf of a number of users it may be sponsored as a bureau. An organisation may submit as a bureau on behalf of users within its own group or for third party customer/clients. In the latter case it is categorised by Bacs as a Bacs Approved Bureau and is subject to a regular, currently triennial, inspection procedure and an annual transaction based charge.

3.2 THE BACS CLEARING PROCESSING CYCLE

The Bacs clearing currently follows a three-day processing cycle, covering three successive bank working days:

Day 1 (Input Day) is the last day for receipt of files if the payments are to be applied on Day 3.

Day 2 (Processing Day) is the day on which payments are passed to the destination banks.

Day 3 (Entry Day) is the day on which all debits and credits, including contra records, are applied to the destination accounts.

A number of reports are produced during the cycle to confirm the arrival and processing of data received. These are described fully in the Bacs user manuals but the two reports, which are always produced and with which users are probably most familiar are:

The **Submission Summary (Arrival) Report** – this electronically transmitted report confirms successful receipt and acceptance of a file submission.

The **Input Report** – this electronically transmitted report confirms the processing of the individual transactions within a file submission. It reflects the validation performed on **Input Day** and details any errors.

A number of other reports, which can be used for auditing purposes, are also available upon request. Details of these and how to obtain them can be found in the Bacs user manuals.

3.3 THE FASTER PAYMENTS DCA CLEARING PROCESSING CYCLE

The DCA module converts items in payment files (Standard 18 format) into single immediate payments (ISO 8583 format), so that any items submitted in the DCA submission window will settle on the same day (i.e. Day 1). Future-dated credits are not accepted.

Reports are produced during the cycle to confirm the arrival and processing of data received. These are described fully in the Faster Payments Service (FPS) user manuals but the two reports with which users are probably most familiar are:

The **Submission Report** – this electronically transmitted report confirms successful receipt of a file submission.

The **Input Report** – this electronically transmitted report confirms the processing of the individual transactions within a file submission, and details any errors or exceptions.

4 THE NEED FOR SECURITY CONTROLS AND PROCEDURES

Information takes a number of forms - it can be stored on computer systems, transmitted across networks, printed out or written down on paper as well as spoken in conversations. Information held and maintained within computer systems, together with any networks that support it, is a particularly important asset. Without it and the computer system on which it is maintained, an organisation may not be able to operate effectively if at all.

Security risks to computer systems are increasing from an ever widening and increasingly sophisticated range of sources. Systems may be the target of a number of threats, including fraud, sabotage, vandalism and other sources of failure as well as natural disasters such as fire and flood. In addition, new sources of potentially damaging threats continue to emerge as well as those already posed by computer viruses and hackers.

All information needs protection from both accidental and deliberate damage and using appropriate security controls and procedures may reduce these risks.

Security controls and procedures combine to cover four areas:

Confidentiality – protecting information from unauthorised disclosure or interception.

Integrity – protecting and ensuring the accuracy and completeness of information and computer systems.

Compliance – ensuring that formalized data procedures are followed at all times in order to reduce risks and to comply with any responsibilities under the Data Protection Act.

Availability – ensuring that information, resources and services, including computer systems, are available when required.

The ***confidentiality***, ***integrity***, ***compliance*** and ***availability*** of an organisation's information are essential in order to maintain its competitive edge, cash-flow, profitability, legal compliance, image and credibility.

Security controls and procedures have four main objectives:

- To prevent security breaches
- To detect a breach if it occurs
- To limit any damage caused by a breach
- To recover from the effects of a breach.

These objectives should be borne in mind when assessing areas of risk within an organisation.

5 RECOMMENDATIONS FOR SECURITY CONTROLS AND PROCEDURES

Bacs and VocaLink take the subject of security very seriously. It accepts responsibility for information received from over 100,000 users together with the processing of over four billion transactions on their behalf. A wide range of security controls and procedures, covering both physical and logical aspects of the processing carried out, are in place to ensure the confidentiality and integrity of user information and the availability of resources to maintain the service.

The procedures operated however, may be to no avail if submissions made are prepared by an organisation where little or no thought has been given to security and where the users themselves cannot be sure of the accuracy and integrity of the information submitted. The systems can validate figures and reconcile totals, but cannot detect fraud or complicity. It is essential that users are confident that the submissions they make are accurate and have been created in an environment where known risks have been identified and addressed.

The recommendations that follow are meant as guidelines and are primarily aimed at organisations that provide Bacs bureau facilities to third party users. They are not all embracing and do not cover every aspect of security. They outline general areas of principle, including examples, relating to Bacs operations and procedures rather than providing a comprehensive security manual. There are many publications available, including the ISO/IEC27002 Code of Practice for Information Security Management, to which the reader may refer for more comprehensive and detailed descriptions of specific security controls, procedures and management.

Some of the recommendations made may not be applicable to the reader's particular environment or set of local circumstances. However, all of them should be considered and used selectively where appropriate according to the potential risk assessed. Most of them are widely accepted by experienced organisations and are often referred to as baseline security controls because they collectively define an industry baseline of good security practice. Some are considered to be of particular importance and are described as key actions or controls, symbolised as a ✓.

The recommendations are organised into a number of categories each of which relates, in general terms, to a functional aspect or operation that is carried out by individual users or bureaux organisations submitting to Bacs.

- Organisation and Policies
- Physical Security
- Computer Operations
- Systems and Applications Support
- Bacs Operations and Procedures

5.1 ORGANISATION AND POLICIES

Organisations that use the Bacs clearing system come in many shapes and sizes with varying degrees of complexity. They range from sole traders to large corporates specialising in the provision of payroll and other financially related services, and from firms of chartered accountants to nation-wide companies offering facilities management services. Most organisations have a set of documented policies and procedures. These describe the organisation's structure and define the rules and regulations that relate to employees. For those organisations that offer customer/client services there is also usually some form of documented contractual arrangement describing the terms and conditions of the services offered.

We recommend that all organisations consider the following aspects of organisation and policies:

5.1.1 SEGREGATION OF DUTIES ✓

Segregation of duties minimises risk of human error, negligence or deliberate system misuse. Consideration should be given to separating duties in order to reduce opportunities for unauthorised modification or misuse of data or services. We recommended that, where possible, the following functions be carried out by separate personnel:

- Customer/client liaison
- Bacs and Bank liaison
- Data entry and control
- Computer operations
- System administration
- Systems development and maintenance
- Change management
- Security administration

Smaller organisations may find this level of segregation difficult to implement, but the principle should be applied as far as is practicable.

5.1.2 EMPLOYMENT CONTRACT AND PERSONNEL POLICIES ✓

Employment contracts are a legal requirement and all employees, whether full-time or part-time, should be issued with and be required to sign a written contract of employment. The contract should include general terms and conditions of employment together with a description of the job. It should also include clauses relating to confidentiality, misuse of computer facilities, security of information, grievance, disciplinary, termination and dismissal procedures. These clauses should be fully detailed as part of the organisation's overall personnel policies and procedures and covered within separate documents, such as an intranet or paper based employee handbook. Where policies are not detailed separately they should be included in each employee's contract of employment. Published procedures, which are followed by all employees, may reduce the probability of litigation through an industrial tribunal.

As a matter of good practice we also recommend that all applicants for employment, including those employed on a contract basis, be screened with references requested and followed up, particularly if the job involves access to systems that contain and maintain sensitive information, particularly of a financial nature.

5.1.3 INFORMATION SECURITY POLICY ✓

This is a policy document, created and maintained by senior management, for all employees and sets out the organisation's commitment to the security of information. The principle objective of the document is to maintain the confidentiality, integrity and availability of the organisation's information.

The policy should contain:

- A definition of information security together with its overall objectives, scope and importance
- A statement of management support and commitment including a note that contravention of the policy may result in disciplinary action
- Specific security principles, standards and compliance requirements, including those relating to the use of the Internet and e-mail facilities
- Individual responsibilities and actions
- The procedures in place for reporting suspected security incidents or breaches
- Responsibilities under and compliance with the terms of the Computer Misuse and Data Protection Acts.

The policy should be subject to regular review and maintenance.

5.1.4 CONTRACTS AND SERVICE LEVEL AGREEMENTS ✓

Organisations that provide services and facilities to third parties generally have some form of legal document agreed and signed by both parties. This may take the form of a contract, letter of engagement or other agreed document that includes general terms and conditions, charges, termination procedures together with a description of the services to be provided. Where third parties also have access to the organisation's IT facilities it is important to identify the potential risks involved and to include security conditions within the contract.

Where an organisation provides payment facilities to third parties through the Bacs clearing it is important to describe those facilities and to define responsibilities relating to both the organisation and the customer/client. This can be achieved either by specifying and defining the responsibilities within the contract or by the use of a Service Level Agreement (SLA) which can be attached to the general contract of those customer/clients making use of the Bacs facilities offered by the organisation. It may also be possible to use the SLA itself as the contractual document.

An example of an SLA, describing a Payroll service, is contained in Appendix. It includes:

- A description of the service provided
- A description of contingency arrangements
- Responsibilities relating to data delivery and verification
- Actions relating to the cancellation of files or transactions
- Actions relating to the checking of the Bacs Input Report.

5.2 PHYSICAL SECURITY

Physical security requirements will vary considerably depending on the size and complexity of the organisation and its IT related operations. Large organisations with purpose built data centres using mainframes have different requirements from those operating server-based equipment from a machine room or using office technology in an open plan environment. Entry systems might, where appropriate, be supplemented with monitoring systems such as alarms and CCTV. However, we recommend that the following general principles be applied in a way that is practical for the organisation.

5.2.1 PHYSICAL ACCESS CONTROL ✓

Entrances to buildings, rooms and offices should be protected by physical entry controls to prevent unauthorised access. Visitors should, ideally, be required to sign-in and out at a reception area and wear a visitor's pass, or other means of identification, and should be accompanied and supervised. Sensitive areas such as computer suites or machine rooms should have additional separate physical access controls. Organisations should also consider retaining and securing visitors' laptops and mobile phones.

Organisations that run their operations from mainframe computers generally secure them, together with peripheral equipment, in a separate computer room or suite. Access to the computer room must always be restricted to authorised personnel and granted, reviewed and maintained in accordance with formalised security procedures. Where access depends on the use of combination codes these should, ideally, be at an individual level and be subject to change control procedures such that they are changed regularly and when an employee leaves or if it is suspected that a code has been compromised.

With the increase use of client/server based configurations it is most important to secure access to the server machines, particularly those on which business applications and customer/client data are held. Many organisations locate their server equipment in a separately secured machine room under much the same security as if it were a mainframe. However, in many cases, because of their relatively compact size, such machines are often located within open plan areas or normal offices with unrestricted access. With the increasing amount of freely available information and software capable of over-riding the security administration levels of proprietary networking software, we recommend that server machines be physically protected with access to them restricted. Similar restrictions should also apply to PCs, either stand alone or networked, which hold sensitive applications and data.

5.2.2 ALARMS

Because of the sensitivity of information held, particularly customer/client information, and the equipment on which it is held, both intruder and smoke detection alarm systems should be used to protect buildings and offices, particularly when they are unoccupied. Such systems should be linked to a monitoring facility. Where offices are sited in or near residential areas the local residents may act in this capacity although we would always recommend a monitored system. Where alarms are coded, change control procedures similar to those used for entry control codes should apply.

Other precautions include employee activated fire alarms and the locating of suitable fire extinguishers. Organisations which run a separate computer suite or machine room should consider the use of specialised fire suppression and environmental control and monitoring devices which should be connected to the alarm system and maintained on a regular basis.

5.2.3 DISPOSAL OF CONFIDENTIAL WASTE ✓

Confidentiality of customer/client information can be compromised through the careless disposal of waste, which may in turn compromise the credibility of the organisation. Consideration should be given to ensuring that such waste, not only on paper but also on computer related media, is destroyed in a secure and certifiable manner. Computer media such as hard drives should also be disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) directive (January 2007) of the Environment Agency.

5.2.4 SCREENING OF PACKAGES

It is an unfortunate reality that packages containing unpleasant or even life threatening substances are sometimes received by organisations. They may not be meant directly for the organisation but are sent to the organisation because it provides services for a third party, which may be the actual target. We recommend ensuring that personnel who open mail receive appropriate training and are aware of the actions to be taken when dealing with letters and packages of a suspect nature.

5.3 COMPUTER OPERATIONS

This section primarily aims to provide recommendations that help safeguard against unauthorised access to computer systems containing an organisation’s business information. It also outlines procedures to help maintain business continuity and to counteract and protect an organisation’s critical processes from the effect of a major failure or disaster.

5.3.1 LOGICAL ACCESS CONTROL AND MONITORING ✓

In the same way as physical security controls are used to restrict and monitor access to a building, so logical access controls are used to control and monitor access to the organisation’s computer systems and resources.

There are four basic stages in the logical access control process:

- Authorisation
- Identification
- Authentication
- Audit

The degree to which these controls are utilised will depend very much upon the number of employees within an organisation who have access to computer resources. For medium and large organisations formal security procedures are considered de facto whereas for smaller businesses with less than say ten employees, such procedures may be considered either impractical or inappropriate. We recommend however that logical access control principles be adopted and applied formally within all organisations and businesses to segregate and protect access to data resources.

Authorisation is the procedure which identifies, controls and monitors who has access to which resources on a computer system or systems and defines how those resources may be used, for example to create, read, write, execute and delete functions. These features are generally included as part of the operating or network system security software. However, in addition, organisations should have formalised procedures that require authorisation access rights to be reviewed and recorded regularly.

Identification is the means by which a user is identified to the system either personally or as part of a group. This code is usually referred to as a “user id” or “account code”. Similar identification codes may be assigned to terminals for recognition when connecting to a central computer. However, “user ids” are not secure as they may be known or shared within an organisation and therefore it is necessary to authenticate the user. There should be a formal user registration and curtailment procedure.

Authentication is the means of confirming the user is actually who they claim to be. This is most commonly achieved by the use of a private secret password maintained by the user. Mainframe operating systems and networks and networked PC systems generally have security software, which facilitates the use and control of passwords, although in some cases these facilities are not fully utilised.

Stand-alone PCs/laptops may be protected using a BIOS or “boot” password facility or utilize specialized security software or the security features of the operating system being used or a combination of these facilities.

5.3.2 PASSWORDS ✓

These can be allocated at several levels within a system in order to prevent access to certain data. Generally this is at system or network level and then again at individual application level. For example a user may be required to logon to a network using a network user identity and password, this may allow the user to choose one of a number of applications which in turn require a separate user id and password in order to gain access. PC systems, which rely on application level passwords only, run the risk of data and software files being corrupted by access through the operating system.

Users should follow good security practices in the selection and use of passwords, which can be defined in an Information Security Policy. The following guidelines are recommended for the allocation and management of passwords -

- Each user should have an individual password to maintain accountability
- Passwords should be kept confidential and not written down
- Passwords should be changed if it is suspected they have become compromised.

Passwords should comprise a minimum of at least eight characters and be complex in structure

- Avoid basing passwords on:
  - Any aspect of the date
  - Family names, car registration, telephone number
  - Company names, identifiers or references
  - User id, user-name, group or system identifier
  - More than two consecutive characters
  - All numeric or all alphabetic.
  - Passwords should be changed at regular intervals and old passwords should not be re-used
  - Temporary passwords should be changed at the first opportunity
  - Passwords should not be coded into any type of automated logon procedure.

The use of complex passwords is particularly encouraged. These comprise eight or more characters, do not contain all or part of the user identifier and contain at least three of the following characteristics – uppercase alphas, lowercase alphas, digits, 0 through 9, and special characters such as !,@,?,#.

Password cracking software uses one of three approaches: intelligent guessing, dictionary attacks and brute force automated attacks that attempt every possible combination of characters. Given enough time, an automated attack can crack any password.

All or some of the above guidelines can be facilitated and enforced automatically by a number of operating and network security software systems. Where such facilities exist we recommend they are used but, where automated procedures are unavailable, we recommend the introduction of written procedures that should be monitored manually.

Audit – is the means of monitoring use of a system by maintaining journals or logs of user activities. As well as recording and logging activities it is particularly useful for identifying potential unauthorised access attempts and for detecting users attempting to access resources for which they are not authorised. Such logging facilities are mainly found on mainframe and networked systems as part of the security system software although software is available which runs on PC systems.

Where such facilities exist we recommend that they be used with the logs reviewed and recorded on a regular basis together with any actions taken.

Other facilities used to reduce the risk of potentially unauthorised access attempts are:

Time-out – this facility automatically logs the user off the system after a specified period of inactivity. This reduces the risk of another, possibly unauthorised user, making use of a session when the terminal or PC is unattended. A number of systems employ a password protected screen-saver facility where the screen is blanked or has a pattern shown after a specified period of time with reactivation and reconnection facilitated by entering a password. A number of systems facilitate a lockout feature activated by the user when the terminal is left unattended, where such a facility is available it should be used.

User disablement – this facility allows a set number, usually three, of incorrect user-id/password combination attempts after which the user-id or terminal or both are disabled. Re-enablement has to be sought from authorised personnel controlled under a formalized procedure. Although in many cases this may be a case of someone forgetting their password, it may also be a potential unauthorised access attempt. Where this facility exists such access attempts should be logged for audit, review and action.

Firewalls and Anti-Virus software – with the increased use of the Internet as a means of gathering and sending information and of doing business, it is vitally important to protect your system, be it a stand-alone PC or a networked system, from the risk of unauthorised external intrusion, which could compromise the confidentiality, integrity and availability of data and information. Firewall and anti-virus Intrusion Detection System devices and software products are readily available to help reduce and control this risk. It should be implemented and regularly maintained wherever such a risk is assessed to be present.

Networks – The majority of network configurations continue to utilize structured cabling for internal local area networks with dedicated private and leased lines or managed networks for linking offices with each other and to the Internet, clients to the bureau and for facilitating wide area networks.

The use of wireless networks, or Wi-Fi as it is commonly referred to, is becoming increasingly popular because of its simplicity and for connecting local computers without the need for cables. Computers connect to the network using radio signals via transmitter/receivers operating under the IEEE 802.1 standards. Wireless connections are facilitated through the use of a Wi-Fi card within the computer or through an external connection linking, wirelessly, to a “hotspot”, which is the common term for the network connection point or wireless access point. Both the Wi-Fi card and the “hotspot” operate under the 802.1 standards.

Wi-Fi Security – “hotspots” can be open or secure. If a “hotspot” is open, then anyone with a Wi-Fi card can access it. If it is secure, the user will require a WEP key to connect. WEP (Wired Equivalent Privacy) is an 802.1 standard encryption system for the radio transmission of data. Whilst secure wireless networks can be detected by outside users they cannot be accessed unless the WEP key is known. However, like passwords, cracking of the WEP key is not impossible and studies have shown that intruders equipped with the proper tools and a moderate degree of technical knowledge could gain unauthorised access. Further security can be gained by disabling the Service Set Identifier (SSID) thereby not broadcasting the name of the wireless network access point.

To address the weaknesses of WEP two new Wi-Fi security certification specifications were developed under IEEE 802.1 for both home and enterprise networks. The latest standard available at the writing of these guidelines is IEEE 802.11i. In 2003 Wi-Fi Protected Access (WPA) was introduced and in 2004 Wi-Fi Protected Access 2 (WPA2), an extended version of WPA was introduced. Each certification provides operation under either an “enterprise” or “personal” mode. The advantage of WPA and WPA2 over WEP is a much higher level of security access control employing sophisticated authentication and encryption technologies.

We currently recommend cabled networks over Wi-Fi networks. Where, however, a Wi-Fi network is used we recommend that users familiarise themselves with the latest IEEE standards and control the use of such networks in accordance with security precautions documented within manufacturer’s documentation together with formalised internal security policies and procedures in order to maintain the highest level of access security to network and data resources.

Basic Wi-Fi security precautions ✓

- Ensure your network is protected with up to date firewall and anti-virus products;
- Always use the highest level of IEEE security standard encryption available;
- Always disable the Service Set Identifier SSID;
- Always force users to access the wireless access point through a user authentication passphrase based on user-id privileges;
- Use Intrusion Detection System devices or software to alert and monitor actual and potential unauthorised intrusions;
- Maintain formalised internal security policies and procedures covering the use of your wireless networks and facilities.

5.3.3 CONTINGENCY, DISASTER AND BUSINESS CONTINUITY PLANNING ✓

The purpose of contingency procedures and disaster recovery plans is to help ensure the continuity and availability of the essential services that an organisation must have in order to continue business. Such procedures and plans must provide, not only for the hardware and software of an organisation’s computer systems, but also for those resources that enable the systems and the organisation to operate, such as personnel, utility services, transport and premises.

Perhaps the most commonly accepted way of maintaining a degree of contingency is to take backups of data, system and application files on a routine basis and especially before and after any major system updates. We recommend that backups are always taken and that they are maintained and rotated on a generation basis sufficient to cover at least the business processing cycle. Backup copies should be held securely both on and off-site and should be tested regularly to ensure usability in the event of a restore being required. Backup master copies of system and application software together with relevant documentation should also be securely retained both on and off-site.

Each organisation faces similar but diverse risks which may impact or cause complete disruption of the business operation, for example equipment failure, accidental or deliberate damage, fire, flood or other natural disaster. It is important that an organisation identifies the potential risks, the extent of their impact on the business and plans accordingly - availability and replacement of PCs is reasonably simple; the same is not true for the availability and replacement of networks and mainframes.

Depending upon complexity, an organisation will require different levels of contingency procedures defined within their disaster recovery and business continuity plans. Each level will have a different focus and may involve different procedures and personnel. A framework for such a plan should include:

Emergency procedures – describing the actions required immediately following a major incident that jeopardises the organisation's business operations and possibly human life.

Fallback procedures – describing the actions required to move the organisation's essential business operations to another location and resume at least a partial service.

Resumption procedures – describing the actions required enabling a return to normal full business operations, usually at the original site.

Test and review procedures – describing how and when plans should be tested and reviewed.

Large organisations tend to have comprehensive plans, which cover all the above procedures and, whilst smaller organisations are less complex, the principles involved should be considered and implemented according to the potential risks identified.

We always recommend that organisations have documented contingency procedures and a disaster recovery plan. These need not be a set of lengthy documents, such documents tend not to be read, but can be a set of simple and straightforward checklists that identify tasks and responsibilities. No matter how well personnel know their jobs, in an emergency they are likely to forget something. Checklists avoid unnecessary stress and help ensure that all aspects of the business are covered.

Another important aspect to bear in mind is that computer equipment, whether mainframe or client/server configuration, needs a constant regulated power supply to maintain operation. Interruptions and loss of power can result in degradation or loss of service and possible corruption of business data. Protection of the power supply should be considered using an Uninterruptible Power Supply, UPS, to ensure at least a controlled close down of operations, or some form of standby generator to enable continued business operations.

A final item, which can sometimes be over-looked, is the need for an adequate level of insurance to cover direct loss of equipment and buildings together with indirect loss due to loss of business revenue. However comprehensive a contingency/disaster recovery plan may be, without the availability of appropriate financial resources, implementation of the plan may not be possible.

5.4 SYSTEMS AND APPLICATIONS SUPPORT

This section looks at the different types and functions of software that are used within an organisation's computer systems environment. It also outlines software support procedures that we recommend in order to minimise the risk of potential disruptions occurring as a result of corruption to the software.

Most computer systems, however simple or complex, usually contain the following categories:

- **Network and operating system software**: this identifies and manages the hardware and software resources that make up the computer system as a whole and enables it to run. The hardware manufacturer or supplier usually provides this type of software. In a number of cases it will include security features that control and audit the use of resources.

- **Firewall and anti-virus products**: these products have become an essential part of the private and corporate computer environment. They help protect against external attacks by filtering, examining and trapping potentially destructive intrusions to your network before they are able to cause disruption. Although sometimes included within the operating system they can also be provided separately by a number of manufacturers in hardware and software formats.
- **Application software**: this is the software that is used to manipulate and maintain an organisation's business data and information. Application software can be developed either by the organisation itself or purchased as a package from an outside supplier. Such software often includes security features that can restrict access both to function and data.
- **Data files/databases/database management systems:** these are associated with all of the above. In the case of application software they are usually the means by which an organisation stores its business data and information.
- The loss of this information can seriously disrupt or prevent an organisation's ability to conduct business. File maintenance is controlled almost exclusively by the application software, which determines the validity of data, applies it in the correct manner and thus maintains the integrity of the information.

5.4.1 NETWORK AND OPERATING SYSTEM SOFTWARE SUPPORT

Upgrades to, or new versions of, network and operating system software tend to be infrequent and users are usually forewarned by the manufacturer well in advance of the release date. However, when upgrades are introduced we recommend they are tested, implemented and recorded in a controlled and monitored manner by authorised personnel complying with formalised change control procedures. Previous versions of the software should also be retained as a contingency measure.

5.4.2 FIREWALL AND ANTI-VIRUS PRODUCTS ✓

These products usually feature facilities, which allow live updates to be conducted automatically although updates can be controlled manually. More complex hardware based firewalls generally require implementation and updating by qualified technical personnel either within the organisation or provided under a maintenance agreement by the manufacturer.

5.4.3 APPLICATION SOFTWARE SUPPORT ✓

Upgrades and new versions of application software, including the maintenance of database management systems, tend to be infrequent and dependent mainly upon statutory and business user requirements.

Where application software and database management systems are provided by an external supplier we recommend the use of similar procedures to those relating to operating system software. User modifications to software packages, apart from user orientated and permitted parameter changes, are usually not permitted as there is no access to the program source code. If amendments become necessary, they are generally provided by the software supplier under a maintenance agreement. This minimises the possibility of amendments being incompatible with future releases.

Where application software is developed and maintained within an organisation, in response to specific business requirements and needs, controls should be in place to minimise the risk of either accidental or deliberate corruption to the software programming code. We recommend the use of a documented development life cycle standard or methodology to control and record any changes or amendments made in a formalized manner. Such methodologies are available from outside suppliers but may also be developed as part of an organisation's internal standards and procedures.

Any organisation developing software to satisfy its own business requirements should have a formalised set of development standards to ensure consistency of approach and quality.

Development standards do not need to be in the form of complex manuals, in fact, in many cases simple and straightforward control documents and checklists are all that is required. However, such documents should be easy to use and provide a consistent and auditable approach.

Development standards should include procedures for:

- Documenting and agreeing business user requirements
- Documenting software specifications
- Thoroughly testing individual programs and all programs together
- Thorough business user testing and acceptance
- Updating user operating instructions and documentation.

Development standards should also include formalised change control management procedures to ensure that:

- Development and testing are carried out on authorised copies of software in a separate testing system environment
- Specifically prepared test data is used with no access to live system data permitted
- Updating to the live system is under written agreement and carried out by authorised personnel only.

Provision should also be made within change control procedures to enable expedient emergency updates or fixes to be implemented under controlled conditions. This may mean reverting to a previous version of the code and for this reason we recommend previous versions be retained.

There is one further category of software, that of **utility software**. This is software that has been developed to perform specific functions across either part of or the whole of the computer system. Utility software programs are usually supplied as part of the operating system software but can also be acquired as separate packages from a number of specialist suppliers depending on the type of function required. Typical examples of this type of software are that of a file editor or a disk space organiser. Some utilities are able to perform very powerful functions and we strongly recommend that strict formalised procedures be adopted to restrict and control their use and to minimise the risk of their possible misuse.

5.5 BACS PROCESSING AND OPERATIONS

This final section describes the four main areas relating to the way in which an organisation receives, creates and submits customer/client data to Bacs:

- **Receipt of customer/client data:** describes the receipt of primary Bacs data and procedures to ensure it is managed correctly.
- **Production of Bacs data:** describes the production of Bacs data files, the conversion of those files into Bacs format and the procedures to ensure its validity and integrity.

- **Submission of Bacs data:** describes the methods of submitting files to the Bacs clearing and the procedures used to ensure it is carried out in a timely and secure manner.
- **Verification of Bacs processing:** describes confirmation and reconciliation procedures to ensure the accuracy of the Bacs processing.

Whilst this section provides recommendations that should be considered in order that potential risks may be reduced, it does not provide details of specific validation facilities and control procedures carried out within the Bacs system, these are to be found in the relevant Bacs Guidance Notes and User Manuals.

5.5.1 RECEIPT OF CUSTOMER/CLIENT DATA ✓

Primary Bacs data, within this context, is defined as being that client data which forms the input to applications that produce transactions, which are subsequently converted to files in Bacs format prior to their submission to the Bacs clearing. Organisations may receive such data from clients in a number of formats. It may be in paper or electronic format. It may be computer generated either by the organisation or directly by the client. It may even be transmitted directly by the client into an organisation’s system. Whichever method of input is used it is important to ensure data validity and integrity in order to prevent the submission of erroneous and possible fraudulent transactions to the Bacs clearing.

Where data is received on paper it is important to ensure that it is keyed correctly and verified against original documentation. Verification should be carried out independently by either another person within the organisation or by the customer/clients themselves. It is also important to ensure that data received has been correctly authorised and that it is applicable to the business cycle being processed. Where misunderstandings arise, or there is difficulty reading or deciphering documents, these should be noted and resolved with the customer/client before any further processing.

With electronic media, as well as checking identification labels and validating contents against customer/client control documents, additional virus checking routines may need to be carried out before any further processing is carried out to ensure the authenticity and integrity of the data.

We recommend that in all cases data received is logged. Special procedures may also be needed to ensure the timely receipt of customer/client data especially if the data processing is subject to a pre-defined timetable such as a payroll run.

Data input directly by customer/clients is usually not under the control of the organisation. However, independent procedures should be in place to ensure the validity, accuracy, completeness and integrity of the data prior to any subsequent processing.

Data generated by an organisation on behalf of its customer/clients should be checked independently and validated prior to any subsequent processing.

In all cases, the client/customer data source should be identified and authenticated. Control reports and schedules utilised to monitor receipt and processing of customer/client data should be auditable. If paper reports are produced they should be initialled and dated by the person responsible, if a computer journal is maintained then the user-id of the person responsible should be recorded. We recommend that, where possible, control reports are sent to customer/clients for authorisation and confirmation before further processing, in which case such authorisation should also be recorded.

5.6 PRODUCTION OF BACS DATA

Before data can be submitted through the Bacs clearing it must be in the specified Bacs file format. This can be achieved by the use of “off-the-shelf” software packages, in-house developed software or a combination of the two. Whichever option is chosen two main processes are involved:

- A process to create a data file of transactions
- A process to convert the data file into a Bacs formatted file.

Procedures relating to these are outlined below but are not intended to cover every combination of how an organisation may operate. They merely provide an example that may be used for comparison.

Once customer/client data have been input and validated the appropriate application software produces a data file. This file contains details of all credit and debit payments to be processed through the Bacs clearing but may not be in the Bacs format. The file is then converted to a file in Bacs format ready for submission.

In many cases production of data files and Bacs formatted files is executed as a single continuous job. This typically occurs where customer/clients input data directly and are responsible for the correctness of the data and the organisation has no responsibility to check it. In other cases the conversion run is executed as a separate job that may take place some time after the production of the data file. This typically occurs where the organisation is responsible for checking data, resolving and correcting any errors or other conditions. An example of this would be the checking of customer/client file and transaction limits. In a number of cases customer/clients require a listing of the transactions on the data file in order to validate them before authorising their submission through the Bacs clearing.

Whichever procedure is employed it is most important to maintain data integrity across the two files. Editing of the files once they have been created should be discouraged, indeed some software packages prevent any access. If it is necessary to access the files this should be restricted to authorised personnel undertaken in accordance with strictly controlled procedures.

Security of Bacs related files ✓

To help maintain data integrity and reduce the risk of possible corruption we recommend that:

- Access to the data and Bacs formatted files is restricted to authorised personnel
- Responsibility for the security of the data and Bacs formatted files is specifically allocated
- Control reports and transaction listings are produced from both the data and Bacs formatted file production runs and independently reconciled and recorded
- Responsibilities relating to the checking and resolution of customer/client data are assigned
- Errors and other conditions, together with customer/client authorisation procedures, are specifically detailed in the customer/client’s contract and Service Level Agreement.

5.6.1 SUBMISSION OF DATA TO THE BACS CLEARING

When Bacs formatted files have been created and relevant reconciliation checks undertaken and recorded, the next step is to submit the file to the Bacs clearing. This is achieved by use of the Bacstel-IP service which is available from 0700 hours Monday* to 2300 hours on Friday* with a

Processing Day cut-off at 22:30-hours each day. The submission window for the Faster Payments Service, known as the Secure-IP service, is 24/7.

There should always be a nominated person or section within the company or organisation with responsibilities for Bacs submissions.

Submissions using the Bacstel-IP service:

This delivery channel is based upon Internet protocols and uses the latest Public Key Infrastructure (PKI) technologies for the highest levels of security. There are two ways to interface with the service:

- Using PKI based Bacs approved software to sign and submit files, maintain reference data and to access and retrieve reports and submission information
- Using a non-PKI based access method via a web browser to access low-risk functions on the Bacs payments services such as accessing reports and maintaining non-sensitive reference data.

Each Bacstel-IP service user, in this case the bureau organisation, must be registered on Bacstel-IP as must all the Bacs service user clients for whom it submits.

✓ Each bureau service user **must have at least two Primary Security Contacts** and may have as many Additional Contacts as deemed necessary. Contacts are those personnel within the bureau authorized under privilege groupings to carry out service functions such as signing and submitting files, accessing reports and maintaining contact details.

PKI uses digital keys and digital certificates to provide security for the submissions. A contact's PKI credentials are made up of their digital keys and their digital certificate and are issued under the authority of the sponsoring Member.

PKI credentials are normally issued and held on a smartcard embedded in a microchip. PKI credentials can also be held on a hardware security module (HSM). An HSM is usually used by an organisation that submits high volumes and requires unattended or automated digital signings and submissions.

✓ The security of the PKI credentials on a smartcard is controlled and maintained by the use of a personal identification number (PIN). The PIN is specific to the smartcard and is issued to the designated contact and **must not be disclosed or shared**.

Similar security measures exist for the operation of HSMs with the exception that once activated, the signing and submission of files is generally fully automated and does not require human intervention until the HSM is shut down.

Non-PKI access is made using the Alternative Security Method (ASM) using a contact ID and password to provide secure access to low-risk functions. A bureau organisation may have as many ASM contacts as is deemed necessary. ASM contacts cannot sign and submit files and cannot maintain sensitive details.

Details relating to the issue, use and maintenance of PKI, HSM and ASM facilities are contained in the Bacstel-IP Service user guide available from the www.bacs.co.uk web site under the Bacstel-IP page.

Submissions using the Secure-IP (FPS) service:

The infrastructure and PKI security supporting the Secure-IP service is similar for DCA submissions as for Bacs submissions. Users should be aware that once files have been submitted the payments contained within them are considered irrevocable. It is therefore most important to ensure the correctness and validity of all files submitted.

Bacs Approved Bureaux can submit files on behalf of corporate clients into the DCA module for same day settlement and these files are treated the same as Bacs files until they reach the DCA module at VocaLink. The main stages are as follows:

- Submission is via Secure-IP, using Bacs approved software, which carries out structural checks and will initially accept or reject the file
- Internal processing at VocaLink disaggregates the file into individual payments, which are then sent to the recipient's bank for credit to account
- Authorisation of corporate payments is carried out by its sponsoring member
- Reporting has two main stages – the **Submission Report** confirms successful receipt of a file submission, and the **Input Report** confirms the processing of the individual transactions within a file submission, and details any errors or exceptions.

Use and security of the Smartcard ✓

Smartcards are issued by Members to each Bacstel-IP contact (Primary Security Contact and Additional Contact) and are used for authenticating the contact to Bacstel-IP and signing payment files prior to submission. The contact must manually enter the smartcard PIN to authorize each signing and submission operation.

It is most important that organisations adopt suitable smartcard management controls covering both the security of the cards and the PINs in accordance with the subscriber policies issued to them by their sponsoring Member. These briefly state that:

- Each smartcard shall be protected by a PIN
- Each smartcard holder shall be responsible for setting and remembering their PIN
- Each smartcard and its PIN shall be secured at all times
- All smartcard activity shall be logged to provide a suitable audit trail
- Smartcards and their associated PIN codes must not be shared.

Business continuity and resilience must be considered with regard to the location and security of smartcards. We recommend that at least one smartcard together with a smartcard reader be retained securely at an off-site location in order to fulfil business continuity requirements in the event of a disaster situation. This should form part of the organisation's disaster recovery plans and procedures – refer 5.3.3 above.

Use and security of the HSM ✓

A number of organisations have a requirement to use HSMs to secure their PKI credentials. Such organisations typically have one or more of the following requirements:

- Large volumes to submit
- Unattended operations

- Complex integration of their own IT infrastructure with Bacstel-IP submissions.

HSMs require more complex security procedures over smartcards due to the wider range of functions supported. HSM contacts are restricted to payment file signing, submission and report retrieval functions only. Management of HSM facilities must be carried out in accordance with the subscriber policies issued to them by their sponsoring Member. These briefly state:

- Any process that alters the state of an HSM, the PKI credentials or manipulates any other sensitive component shall be formalised in a Key Management procedure
- All procedures shall be documented and be subject to change control
- All procedures carried out shall be carried out by authorized personnel
- A Key Management log shall be maintained to record details of changes in an auditable form
- Key Management logs shall be maintained securely to ensure unauthorized modification is not possible.

Consideration should be given to applying dual control to any or all of the above procedures.

HSM user organisations should also ensure a minimum of the following organisational roles:

- Key Manager – having overall responsibility for Key Management operations within the organisation and ensuring compliance with Key Management procedures
- Physical Security Manager – having responsibility for managing those facilities which provide physical security to the environment where HSM devices are located
- Application Administrator – having responsibility for managing the Bacstel-IP application platform
- Auditor – having responsibility for the review of all key and certificate activities to verify that they have been carried out in line with subscriber policies.

Business continuity and resilience should be considered with regard to supporting:

- Backup keys – whilst this may provide protection it may incur additional infrastructure cost. In the event of a key/certificate being rendered unusable, the organisation may elect to perform operations manually by use of smartcards
- Cloned keys – where resilience is required to support unattended operations it may be necessary to clone keys to an equivalent device for use in the operational environment resulting in two or more HSM devices holding the same keys
- Multiple keys – greater resilience is achieved where an organisation supports multiple keys across multiple HSM devices.

The subscriber policies mandate no specific procedures but whichever approach is adopted it should form part of the organisation’s disaster recovery plans and procedures – refer 5.3.3 above.

✓ **Recording** – formalised procedures should be in place in order to record and reconcile details relating to each Bacs submission. Details recorded should include the client details together with the Bacs processing date and number and value of items. The details should be used for reconciliation against the control reports produced by the Bacs related applications and the reports received from Bacs.

Recall – appropriate procedures should be in place to enable the recall or extraction from processing of submitted files, when requested by a customer/client. Responsibilities for such action should be specified in the customer/client’s contract and SLA.

5.6.2 VERIFICATION OF BACS PROCESSING

Files may be submitted to Bacs up to 31 days in advance of the **Processing Day**. On arrival, all files submitted are read to determine they conform to Bacs formatting standards. Files are held on a suspense system until the **Input Day** when a full validation check is undertaken to ensure the validity of the data including destination bank sort codes, file and transaction limits.

On the **Processing Day** the individual transactions contained within the files are processed to the individual banks.

Reports are produced and sent by Bacs to organisations in order for them to monitor the progress and accurate processing of their submissions. These reports comprise:

- An on-line **Submission Summary (Arrival) report** providing on-line acknowledgement that the submission has been accepted by Bacs and has passed preliminary checks. The report includes details of the following information -

  - Bureau details
  - Date of the transmission
  - Bacs processing date
  - Number and value of items.

- An on-line **Rejection report** is produced if a file is rejected as a result of a validation error.
- Only credit items with an individual maximum limit, designated by the sponsoring bank, can be submitted via DCA and these items cannot be future dated, as they must be for same-day settlement.

✓ **Report Checking and Reconciliation** - formalised procedures should be in place to check and validate the contents of the Bacs Submissions Summary reports and to reconcile them to control totals recorded prior to the submission. Such procedures should include the checking and reconciliation of:

- File header and trailer data
- Number and value of records.
- Such procedures should also include the recording and resolution of:
- Rejection Report errors
- Transmission failure.

✓ The Input Report confirms the processing of a submission to Bacs. It is the prime checking document and should be subject to thorough inspection according to formalised procedures.

The Input Report details:

- File header and trailer data
- Amended and rejected records
- Number and value of records
- Transaction account totals and account limit values for the period
- Credit transactions in excess of maximum value limit
- Sample data (if applicable)
- File authentication check total (if applicable).

✓ **Report Checking and Reconciliation** – formalised procedures should be in place to ensure the timely collection of the Bacs reports, including the Input Report, to check and validate their contents and to reconcile appropriate control totals recorded prior to the submission.

Bacs recommends that customer/clients collect their own Bacs reports in order that they may carry out validation and reconciliation checks. However, where a customer/client requests that reports be collected by the bureau organisation it is most important that the checks carried out, especially in relation to the checking of amounts in excess of predefined limits, together with the resolution of any unusual and error conditions, are specified in each customer/client's Service Level Agreement (SLA) - refer section 5.1.4 above.

Where the customer/clients collect their own Bacs reports, including the Bacs Input report, directly from the Bacs Payment Services web site, it is important to specify what they should be checking and how details should be validated and reconciled. It is also important that clients be made aware of what action is needed if their reports are not available. These details should all be specified in each customer/client's Service Level Agreement (SLA) - refer section 5.1.4 above.

6 SUMMARY

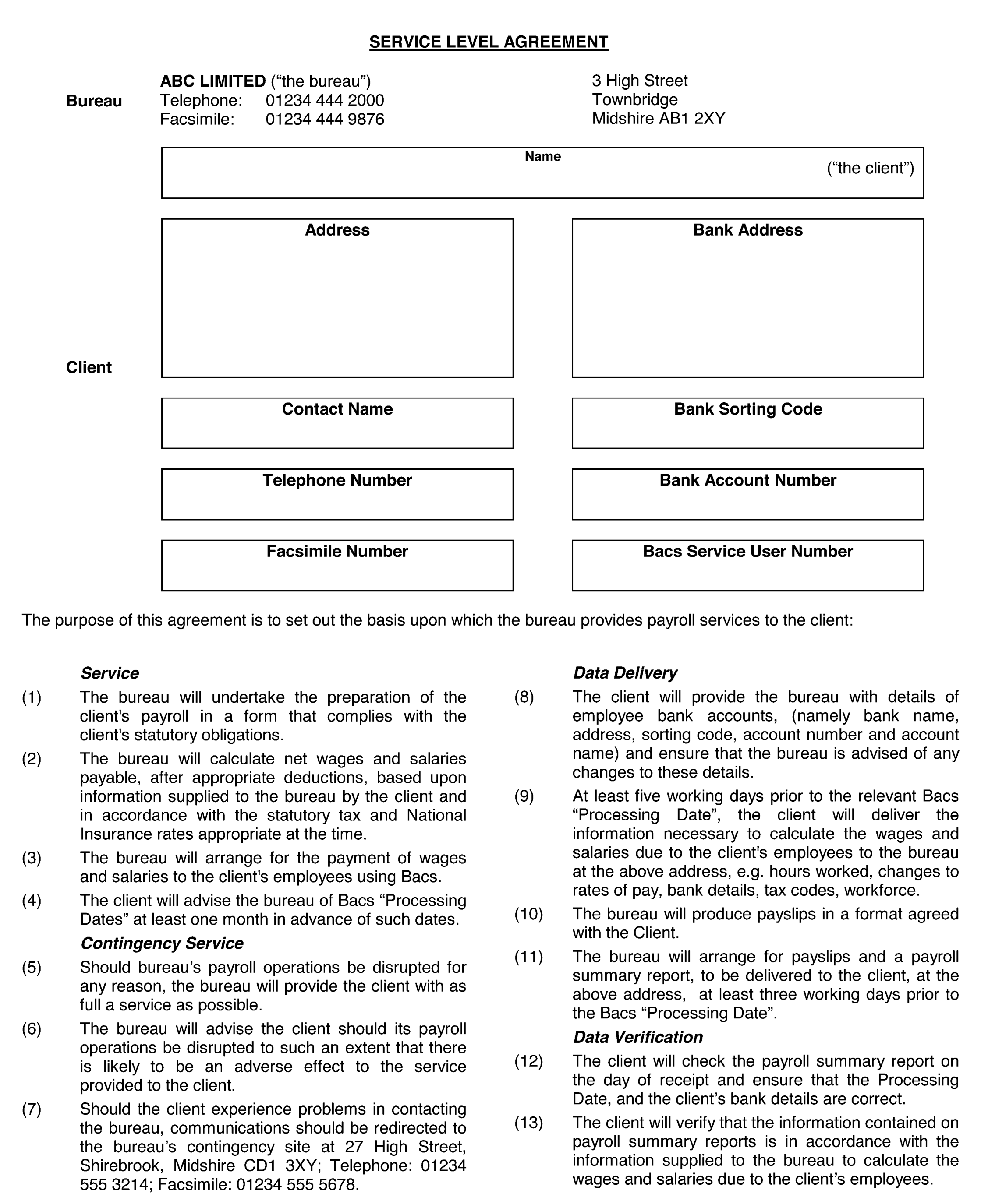
The purpose of these guidelines has been to provide the reader with an awareness of the potential areas of risk within an organisation providing Bacs related services together with controls and procedures that we believe can be implemented to reduce those risks. The recommendations made should be considered within the structure and framework of an organisation according to its size and complexity of operation. However, we do recommend that the controls and procedures described, particularly those described as key, be considered and implemented where appropriate and reviewed on a regular basis.

The ***key*** controls described are:

✓ Staff contract and personnel policies
✓ Information Security Policy
✓ Contracts and Service Level Agreements
✓ Physical access control
✓ Passwords
✓ Contingency, disaster and business continuity planning
✓ Security of the Bacs related files
✓ Use and security of the Smartcard
✓ Use and security of the HSM
✓ Recording and reconciling data submitted to Bacs
✓ Receipt, checking and reconciliation of Bacs reports.

It is now an accepted fact that the ever changing and increasingly frequent updates and advances in technology impact not only on the way in which we work, but also in the way we must deal with additional potential risks to our systems. Even so, the principles outlined in this document should provide organisations with a basis from which to implement and develop their own risk assessment, management and reduction control processes.

7 APPENDIX



SERVICE LEVEL AGREEMENT

Bureau

ABC LIMITED ("the bureau")
Telephone: 01234 444 2000
Facsimile: 01234 444 9876

3 High Street
Townbridge
Midshire AB1 2XY

Client

Name ("the client")

Address

Bank Address

Contact Name

Bank Sorting Code

Telephone Number

Bank Account Number

Facsimile Number

Bacs Service User Number

The purpose of this agreement is to set out the basis upon which the bureau provides payroll services to the client:

Service

(1) The bureau will undertake the preparation of the client's payroll in a form that complies with the client's statutory obligations.

(2) The bureau will calculate net wages and salaries payable, after appropriate deductions, based upon information supplied to the bureau by the client and in accordance with the statutory tax and National Insurance rates appropriate at the time.

(3) The bureau will arrange for the payment of wages and salaries to the client's employees using Bacs.

(4) The client will advise the bureau of Bacs "Processing Dates" at least one month in advance of such dates.

Contingency Service

(5) Should bureau's payroll operations be disrupted for any reason, the bureau will provide the client with as full a service as possible.

(6) The bureau will advise the client should its payroll operations be disrupted to such an extent that there is likely to be an adverse effect to the service provided to the client.

(7) Should the client experience problems in contacting the bureau, communications should be redirected to the bureau's contingency site at 27 High Street, Shirebrook, Midshire CD1 3XY; Telephone: 01234 555 3214; Facsimile: 01234 555 5678.

Data Delivery

(8) The client will provide the bureau with details of employee bank accounts, (namely bank name, address, sorting code, account number and account name) and ensure that the bureau is advised of any changes to these details.

(9) At least five working days prior to the relevant Bacs "Processing Date", the client will deliver the information necessary to calculate the wages and salaries due to the client's employees to the bureau at the above address, e.g. hours worked, changes to rates of pay, bank details, tax codes, workforce.

(10) The bureau will produce payslips in a format agreed with the Client.

(11) The bureau will arrange for payslips and a payroll summary report, to be delivered to the client, at the above address, at least three working days prior to the Bacs "Processing Date".

Data Verification

(12) The client will check the payroll summary report on the day of receipt and ensure that the Processing Date, and the client's bank details are correct.

(13) The client will verify that the information contained on payroll summary reports is in accordance with the information supplied to the bureau to calculate the wages and salaries due to the client's employees.

Bacs provides this document without responsibility. It is purely an example of a Service Level Agreement. Whilst organisations are free to copy this document, they should satisfy themselves as to its suitability for their specific organisation.

(14) The client will check the payroll summary report to ensure that:

- The number of transactions equate to the number of the client's employees;
- The total value of payments is in line with the clients' normal wages and salaries for the period involved;
- That the total value of payments does not exceed the limit negotiated with the client's Bacs sponsor;
- No single payment is exceptional, after taking account of overtime and special payments or bonuses;
- No more than one payment is destined for the same account, except where more than one employee shares a joint account.

(15) The client will inform the bureau of any errors identified on payroll summary reports no later than 12 noon on the day of receipt.

Cancellation of Payments

(16) The client will arrange the cancellation of individual payments by contacting their Bacs sponsor.

(17) If it is necessary to withdraw the whole Bacs file, the client will contact the bureau before 3pm on Input Day.

Bacs Input Report

(18) This report provides details of the payments that have been sent electronically to the Bacs service on behalf of the client. The client must collect their copy of the input report via the Internet following email notification from the Bacs service.

(19) If the client is unable to collect their Bacs Input Report for any reason, they must contact their Bacs sponsor before 11am on Processing Day for verification of the Bacs transmission.

(20) The client will check the Bacs Input Report to:

- Ensure the Service User Number and User Name in the main heading block of the report reflect the client's registration with Bacs;
- Ensure that both the number and value of payments agree with the payroll summary report forwarded to the client by the bureau;
- Ascertain details of any rejected or adjusted records.

(21) The client is responsible for dealing with any rejected or adjusted records identified in the Bacs Input Report.

(22) The client must immediately advise their Bacs Sponsor, and the bureau, of any errors identified on the Bacs Input Report.

Signed for and on behalf of the Bureau:

....

Bureau

Name: ....

Position: ....

Date: ....

Signed for and on behalf of the Client:

....

Client

Name: ....

Position: ....

Date: ....

DEFINITIONS:

Bacs — The electronic funds transfer system operated by VocaLink Limited on behalf of Bacs Payment Schemes Limited**.**

Bacs Sponsor — The bank or building society sponsoring the client to use the Bacs service

Bacs Processing Cycle — The three consecutive working days in the Bacs Processing Cycle are:

- Day 1 - Input Day (the last day when the file may be received by the Bacs service);
- Day 2 - Processing Day;
- Day 3 - Debit/Credit Day (the day when items should reach destination).

Bacs® is a registered trademark of Bacs Payment Schemes Limited

Bacs provides this document without responsibility. It is purely an example of a Service Level Agreement. Whilst organisations are free to copy this document, they should satisfy themselves as to its suitability for their specific organisation.