



SARK UCS/MVP TDM/IP PBX Advanced Voice Recording (AVR)

**SARK UCS/MVP Version 2 Release 2
January 2010**

Table of Contents

<u>SARK UCS/MVP recording; modes of operation and system defaults.....</u>	<u>3</u>
<u>Recording settings.....</u>	<u>3</u>
<u>Recording process.....</u>	<u>3</u>
<u>Setting Recording options for a user.....</u>	<u>3</u>
<u>Telephone Recording – legal requirements.....</u>	<u>4</u>
<u>Ofcom FAQ on voice recording.....</u>	<u>4</u>
<u>“LBP Regulations”</u>	<u>6</u>

SARK UCS/MVP recording; modes of operation and system defaults

Recording settings

MONITOROUT=/home/e-smith/files/primary/files/monout
MONITORSTAGE=/home/e-smith/files/primary/files/stage
MONITORTYPE=tmpfs
RECQDITHER=2
RECQITDELAY=30
RECQSEARCHLIM=200
RECRSYNCPARMS=

Default recording mode NONE

Recording options available:-

- Inbound
- Outbound
- Both
- OTRR

Recording process

All voice capture is done directly to tmpfs in main memory. Immediately after a recorded call ends, a task is called to off-load the recording from memory to a staging dataset (MONITORSTAGE). Every minute, a cron job examines the off-loaded directory, does some housekeeping on the recorded files and moves them to the output staging directory (MONITOROUT). Every hour, a cron rsync job starts and moves recorded files from the output staging directory to the NAS/NFS device. Rsync will save the recordings into directories organized by date; so for example, recordings made on the 4th July 2010 will be stored in a directory called *04072010*.

Recordings are named as follows:-

{Linux Epoch}-{DNID}-{CLID}.wav

A real example calling from extension 5099 to a test number; 01924 566170, looks like this

1263728106-01924566170-5099.wav

Setting Recording options for a user.

Recording options for individual extensions can be set by editing the *RecOpts* value in the extensions entry. If you intend to use OTRR then the activation DTMF is *1. You should set this as a button on the phone because Asterisk only allows 30 milliseconds between key-presses which makes it tricky to enter manually.

Telephone Recording – legal requirements

You should be aware that there are legal implications whenever you record a call and that neither Aelintra nor its distributors or resellers will be responsible in the event that you use the recording software in an unlawful manner. Below are included some reprints which you may find useful, however if you are in any doubt regarding the legality of your proposed recordings then you should seek legal advice *before* you begin.

Ofcom FAQ on voice recording

Reproduced from

<http://www.ofcom.org.uk/static/archive/oftel/consumer/advice/faqs/prvfaq3.htm>

Recording and monitoring telephone calls or e-mails

A general overview of interception, recording and monitoring of communications

The interception, recording and monitoring of telephone calls is governed by a number of different pieces of UK legislation. The requirements of all relevant legislation must be complied with. The main ones are:

- Regulation of Investigatory Powers Act 2000 ("RIPA")
- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 ("LBP Regulations")
- Data Protection Act 1998
- Telecommunications (Data Protection and Privacy) Regulations 1999
- Human Rights Act 1998

It is not possible to provide comprehensive detail of that legislation here. Any person considering interception, recording or monitoring of telephone calls or e-mails is strongly advised to seek his/her own independent legal advice and should not seek to rely on the general information provided below. It should be borne in mind that criminal offences and civil actions may occur when the relevant legislation is not complied with. Accordingly, Oftel accepts no liability for reliance by any person on the following information.

Can I record telephone conversations on my home phone?

Yes. The relevant law, RIPA, does not prohibit individuals from recording their own communications provided that the recording is for their own use. Recording or monitoring are only prohibited where some of the contents of the communication - which can be a phone conversation or an e-mail - are made available to a third party, ie someone who was neither the caller or sender nor the intended recipient of the original communication. For further information see the [Home Office website](#) where RIPA is posted.

Do I have to let people know that I intend to record their telephone conversations with me?

No, provided you are not intending to make the contents of the communication available to a third party. If you are you will need the consent of the person you are recording.

Can a business or other organisation record or monitor my phone calls or e-mail correspondence with them?

Yes they can, but only in a limited set of circumstances relevant for that business which have been defined by the LBP Regulations. The main ones are:

- to provide evidence of a business transaction
- to ensure that a business complies with regulatory procedures
- to see that quality standards or targets are being met in the interests of national security
- to prevent or detect crime to investigate the unauthorised use of a telecom system
- to secure the effective operation of the telecom system.

In addition, businesses can monitor, but not record, phone calls or e-mails that have been received to see whether they are relevant to the business (ie open an employee's voicemail or mailbox systems while they are away to see if there are any business communications stored there). For further information see the [DTI website](#) where the LBP Regulations are posted.

However any interception of employees' communications must be proportionate and in accordance with Data Protection principles. The Information Commissioner has published a Data Protection Code on "Monitoring at Work" available on its website [here](#). The Code is designed to help employers comply with the legal requirements of Data Protection Act 1988. Any enforcement action would be based on a failure to meet the requirements of the act - however relevant parts of the Code are likely to be cited in connection with any enforcement action relating to the processing of personal information in the employment context. Accordingly this Code of Practice and the Data Protection Act must also be considered by any business before it intercepts employees' communications.

Do businesses have to tell me if they are going to record or monitor my phone calls or e-mails?

No. as long as the recording or monitoring is done for one of the above purposes the only obligation on businesses is to inform their own employees. If businesses want to record for any other purpose, such as market research, they will have to obtain your consent.

What do I do if my calls have been recorded unlawfully?

Under RIPA it is a tort to record or monitor a communication unlawfully. This means that if you think you have suffered from unlawful interception of your phone calls or e-mails you have the right to seek redress by taking civil action against the offender in the courts.

(If you have been following the steps to contact Ofcom and this FAQ has not helped then proceed to [Step 3](#))

“LBP Regulations”

Below is a copy of the LBP regulations referred to in the Ofcom FAQ. It is useful because in addition to the regulations covering the lawful interception of communications, it also includes an explanatory note which you might find helpful.

Statutory Instrument 2000 No. 2699

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

© Crown Copyright 2000

Statutory Instruments printed from this website are printed under the superintendence and authority of the Controller of HMSO being the Queen's Printer of Acts of Parliament.

The legislation contained on this web site is subject to Crown Copyright protection. It may be reproduced free of charge provided that it is reproduced accurately and that the source and copyright status of the material is made evident to users.

It should be noted that the right to reproduce the text of Statutory Instruments does not extend to the Queen's Printer imprints which should be removed from any copies of the Statutory Instrument which are issued or made available to the public. This includes reproduction of the Statutory Instrument on the Internet and on intranet sites. The Royal Arms may be reproduced only where they are an integral part of the original document.

The text of this Internet version of the Statutory Instrument which is published by the Queen's Printer of Acts of Parliament has been prepared to reflect the text as it was Made. A print version is also available and is published by The Stationery Office Limited as the **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**, ISBN 0 11 099984 3. The print version may be purchased by clicking [here](#). Braille copies of this Statutory Instrument can also be purchased at the same price as the print edition by contacting TSO Customer Services on 0870 600 5522 or e-mail:customer.services@tso.co.uk.

Further information about the publication of legislation on this website can be found by referring to the [Frequently Asked Questions](#).

To ensure fast access over slow connections, large documents have been segmented into "chunks". Where you see a "continue" button at the bottom of the page of text, this indicates that there is another chunk of text available. 

STATUTORY INSTRUMENTS

2000 No. 2699

INVESTIGATORY POWERS

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<i>Made</i>	<i>2nd October 2000</i>
<i>Laid before Parliament</i>	<i>3rd October 2000</i>
<i>Coming into force</i>	<i>24th October 2000</i>

The Secretary of State, in exercise of the powers conferred on him by sections 4(2) and 78(5) of the Regulation of Investigatory Powers Act 2000^[1] ("the Act"), hereby makes the following Regulations: -

Citation and commencement

1. These Regulations may be cited as the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and shall come into force on 24th October 2000.

Interpretation

2. In these Regulations -

(a) references to a business include references to activities of a government department, of any public authority or of any person or office holder on whom functions are conferred by or under any enactment;

(b) a reference to a communication as relevant to a business is a reference to -

(i) a communication -

(aa) by means of which a transaction is entered into in the course of that business, or

(bb) which otherwise relates to that business, or

(ii) a communication which otherwise takes place in the course of the carrying on of that business;

(c) "regulatory or self-regulatory practices or procedures" means practices or procedures -

(i) compliance with which is required or recommended by, under or by virtue of -

(aa) any provision of the law of a member state or other state within the European Economic Area, or

(bb) any standard or code of practice published by or on behalf of a body established in a member state or other state within the European Economic Area which includes amongst its objectives the publication of standards or codes of practice for the conduct of business, or

(ii) which are otherwise applied for the purpose of ensuring compliance with anything so required or recommended;

(d) "system controller" means, in relation to a particular telecommunication system, a person with a right to control its operation or use.

Lawful interception of a communication

3. - (1) For the purpose of section 1(5)(a) of the Act, conduct is authorised, subject to paragraphs (2) and (3) below, if it consists of interception of a communication, in the course of its transmission by means of a telecommunication system, which is effected by or with the express or implied consent of the system controller for the purpose of -

(a) monitoring or keeping a record of communications -

(i) in order to -

(aa) establish the existence of facts, or

(bb) ascertain compliance with regulatory or self-regulatory practices or procedures which are -

applicable to the system controller in the carrying on of his business
or

applicable to another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures, or

(cc) ascertain or demonstrate the standards which are achieved or

ought to be achieved by persons using the system in the course of their duties, or

(ii) in the interests of national security, or

(iii) for the purpose of preventing or detecting crime, or

(iv) for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system, or

(v) where that is undertaken -

(aa) in order to secure, or

(bb) as an inherent part of,

the effective operation of the system (including any monitoring or keeping of a record which would be authorised by section 3(3) of the Act if the conditions in paragraphs (a) and (b) thereof were satisfied); or

(b) monitoring communications for the purpose of determining whether they are communications relevant to the system controller's business which fall within regulation 2(b)(i) above; or

(c) monitoring communications made to a confidential voice-telephony counselling or support service which is free of charge (other than the cost, if any, of making a telephone call) and operated in such a way that users may remain anonymous if they so choose.

(2) Conduct is authorised by paragraph (1) of this regulation only if -

(a) the interception in question is effected solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller's business;

(b) the telecommunication system in question is provided for use wholly or partly in connection with that business;

(c) the system controller has made all reasonable efforts to inform every person who may use the telecommunication system in question that communications transmitted by means thereof may be intercepted; and

(d) in a case falling within -

(i) paragraph (1)(a)(ii) above, the person by or on whose behalf the interception is effected is a person specified in section 6(2)(a) to (i) of the Act;

(ii) paragraph (1)(b) above, the communication is one which is intended to be received (whether or not it has been actually received) by a person using the telecommunication system in question.

(3) Conduct falling within paragraph (1)(a)(i) above is authorised only to the extent that Article 5 of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector^[2] so permits.

Patricia Hewitt,
Minister for Small Business and E-Commerce, Department of Trade and Industry

2nd October 2000

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations authorise certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers Act 2000. To the extent that the interceptions are also prohibited by Article 5.1 of Directive 97/66/EC, the authorisation does not exceed that permitted by Articles 5.2 and 14.1 of the Directive.

The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions) for purposes relevant to that person's business and using that business's own telecommunication system.

Interceptions are authorised for -

monitoring or recording communications -

to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training),

in the interests of national security (in which case only certain specified public officials may make the interception),

to prevent or detect crime,

to investigate or detect unauthorised use of telecommunication systems or,

to secure, or as an inherent part of, effective system operation;

monitoring received communications to determine whether they are business or personal communications;
monitoring communications made to anonymous telephone helplines.

Interceptions are authorised only if the controller of the telecommunications system on which they are effected has made all reasonable efforts to inform potential users that interceptions may be made.

The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented: they are not prohibited by the Act.

A regulatory impact assessment is available and can be obtained from Communications and Information Industries Directorate, Department of Trade and Industry, 151 Buckingham Palace Road, London SW1W 9SS. Copies have been placed in the libraries of both Houses of Parliament.

Notes:

[1] 2000 c. 23.[back](#)

[2] O.J. No. L24, 30.1.98, p.1.[back](#)
