Water distribution WSP	**Unauthorised access to the network** *Management/technical guidance*	

Information derived from:	**Related tools:**
○ Feedback from water suppliers	○ Network design & modelling ○ Stakeholder management ○ Finance and charging

Important Notes to users:

This document provides information to support improved management of piped drinking water quality by water utilities and other stakeholders. It cannot however be definitive and users must ensure that they assess local factors and particularly take account of any national or regional legislative requirements before use. Where necessary this may also need close collaboration with others. The priority to be given to implementing controls to manage identified water quality risks will depend on a proper prioritisation process by each water supplier.

Summary

It is the experience of many water suppliers that illegal or unauthorised access to the distribution network can occur for a variety of reasons. This poses a number of water quality risks and can also create wider problems related to loss of revenue. This document briefly summarises the water quality risks associated with unauthorised access and how they can be mitigated.

Detailed information

Background

Illegal or unauthorised access to the distribution network can arise from time to time in many water supply systems but the problem can often be particularly acute in some developing countries. Reasons include vandalism, use of the water for commercial activity and building, and use by those who do not have access to or cannot afford piped supplies.

Water quality risks

The water quality risks relate mainly to ingress of contaminants. The risks can be significantly increased if the unauthorised access occurs in an area where major sources of contamination exist for example in areas with poor sanitation arrangements. The risks can occur from both:

- Direct backsiphonage of a range contaminants at the point of access including faecal matter, industrial chemicals and other material
- Indirectly by reducing water pressure thus increasing the risk of backsiphonage elsewhere in the local vicinity

Also if the volume of water taken is significant, then this can adversely affect the overall operation of the distribution network by changing flow rates and direction.

Risk mitigation measures

Dealing with unauthorised or illegal access can be difficult but typically relies on two main approaches:

- Security
  Points at which access is typically made include valve chambers or fire hydrants. This can be made more difficult by measures such improved and more secure design of valve chambers and lockable or special design fire hydrant covers.
- Education
  Where it is appropriate to allow access to the network by third parties, for example for fire authorities and builders then this should be conditional on proper training and possibly certification. More generally in areas where unauthorised access is common then a programme of local community education could be established to highlight the risks.

Typical control points

Typically the two main control points are:

- Inspection
  The easiest to implement is regular inspection of the network to identify points at which unauthorised access regularly occurs so that the appropriate authorities can be notified and action taken. Where third parties have been authorised to use the network then such use should be inspected to ensure that proper procedures are being used.
- Network pressure
  If network pressure loggers or monitoring exists then this can also be used to identify points at which pressure is regularly reduced for unexplained reasons.

Reference for further detailed information:

- Relevant case studies

Typical resources needed:

The resources necessary will vary considerably. Routine inspection can be integrated into awareness training of all utility staff. The extent to which additional security and structured stakeholder engagement and training are justified will depend on a local assessment of the risks and benefits.

Document creation:

Author	**Date**
Bob Breach	August 2009