



NETconsent Whitepaper

Communicating Corporate Policies

Table of Contents

| | |
|---|----|
| Introduction | 3 |
| Traditional Policy Deployment Methods | 4 |
| NETconsent Solution History | 5 |
| Information Commissioner’s Recommended Guidelines | 5 |
| NETconsent Technology: Policy Enforcement Points | 6 |
| Mandatory and Non Mandatory Policies | 8 |
| Recommended Implementation | 9 |
| Technical Deployment | 10 |
| About NETconsent | 11 |

Introduction

Organisations have published corporate policies and procedures for many years. However the pace of change in key areas, such as legislation, organisational culture and technological developments increasingly requires organisations to revise their policies and procedures more frequently and provide auditable processes to demonstrate good corporate governance.

This whitepaper reviews the traditional methods available to create, publish and distribute corporate policies and an alternative automated approach designed to ease the administrative burden of policy deployment and enforcement.

Traditional Policy Deployment Methods

When applied consistently within an organisation, policies and procedures promote a positive work environment, as everyone understands their rights and responsibilities.

Historically an organisation with thousands of staff and hundreds of policies in areas such as HR, health & safety and professional conduct has had to struggle with paper-based systems. These range from employee handbooks, inserts within payslips, memos and staff notice boards. Inevitably this has led to a time intensive, laborious and error prone process.

More recently the use of email and Intranet sites has eased the burden for some organisations when publishing policies, however these methods do not generally assist with the collection of users' agreement to be bound by those policies.

Many organisations still do not track employees' consent to official corporate and legal policies which makes it difficult to take legitimate disciplinary action when policies are breached by employer or employee.

NETconsent streamlines the process to ensure that all policies are effectively delivered and helps to maintain the all important audit trail. Not only can an IT based policy management strategy save time and money through operational efficiencies, it will also assist the board to demonstrate good Corporate Governance.

Organisations are able to prove that relevant and up to date policies have been consistently distributed to all employees. Organisations can easily show who has read and agreed to the latest revision of a policy, which helps protect the employer and employee.

Typically organisations have between 50 to 150 policies and procedures and although not all may require formal acceptance, it is important that all policies are read and then stored in a central location to revisit if required.

There are a number of questions to consider:

- Do employees know which policies are relevant to them? Do they later find that they have contravened a policy they were not aware of?
- If policies are displayed on Intranet sites or in the Employee Handbook, how does an organisation demonstrate which policy version has been read? And when?
- How do you ensure that temporary staff and contractors are aware of where policies are stored and which ones are relevant?
- Are employees able to decline a policy if they are unsure of the context or have further questions?

Following the authoring and review process of any policy, it is estimated that the cost to an organisation of manual deployment is in excess of £10 per user per policy version. This estimate includes both visible and hidden costs such as paper, printing, postage, clerical administration, storage and reporting costs.

NETconsent Solution History

The prototype of NETconsent was developed in 2000 under the name of "I Agree". I Agree was developed for Manor Bakeries, to facilitate the dissemination of a new Web Acceptable Usage Policy (AUP) preceding the implementation of a URL filtering software solution.

Prior to the introduction of Internet Access Control Software, it was deemed necessary to notify users of the organisation's usage Policy, including the user's responsibilities as well as the monitoring and auditing principles being implemented. The brief was to restrict users from accessing the Internet until users had formally agreed to abide by the AUP. Agreement needed to be logged into a database specifying the version(s) of each new revision of policy, thereby providing an audit trail for later use.

Manor Bakeries' requirements were in line with The Data Protection Act 1998 which came into force on 1st March 2000. Guidelines later introduced by the Information Commissioner in his third part of the Employment Practices Data Protection Code – "Monitoring at Work" further clarified the Act.

Information Commissioner's Recommended Guidelines

The Information Commissioner's supplementary guidance to Part 3 of the Employment Practices Data Protection Code provides clear and practical guidance for employers about monitoring employees in the work place. (<http://www.informationcommissioner.gov.uk>)

Richard Thomas, Information Commissioner said:

"Part 3 of the Employment Practice Data Protection Code aims to strike a balance between the needs of employees and the rights of employees. If an employer has to check how staff are using computers at work, he should make sure they know how and why checks will be carried out. If any monitoring is to take place it must be open and transparent and with the knowledge of the employee."

The code states:

"The capabilities of electronic systems should be used to remind workers of their responsibilities. These can be set so that workers cannot proceed to access the internet or e-mail services without acknowledging the acceptance of certain conditions."

The Information Commissioner also goes on to say that an organisation must be able to demonstrate beyond all reasonable doubt that an individual has been given the opportunity to see and accept the policy.

The key word here is *opportunity* and it does not mention the "understanding". In another excerpt, the topic of understanding is discussed and it clearly says that human interaction should be used to ensure users understand the content of the policies and the way in which an organisation will manage against the policies.

NETconsent Technology: Policy Enforcement Points

NETconsent works using a technology called Policy Enforcement Points (PEP). PEPs are distributed around the network at various IT access points such as LAN, E-MAIL, WEB and Extranets. When a user tries to access any of these services, the NETconsent Policy Engine checks for new or updated policies, if there are new policies to be agreed to the NETconsent Policy Kiosk is displayed.

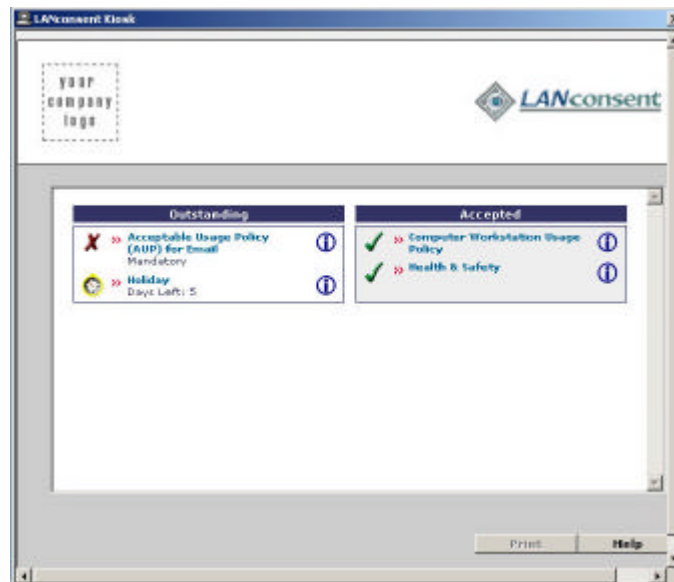


Diagram: The NETconsent Policy Kiosk

If the Kiosk is displayed, the user will know that there is a new policy (or multiple policies) to agree to. If there are no new or updated policies or procedures to be processed, the user will not be presented with this screen.

To agree to be bound by a policy, the user is required to select a policy from the outstanding list. The chosen policy's content is displayed to the user, who is able to accept or decline the policy, by scrolling to the end and clicking a button. This action demonstrates that the complete wording has passed the user's eyes.

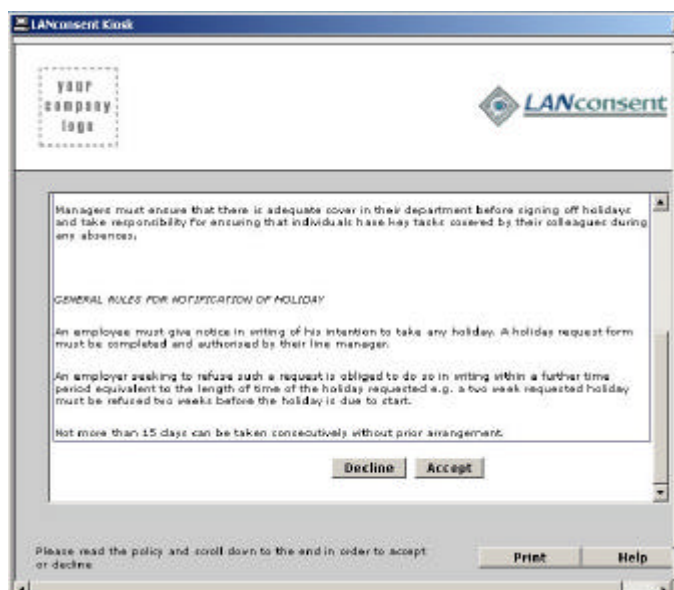


Diagram: The Policy Acceptance Screen displayed to users

Once the user has clicked on the Accept button, they are asked to authenticate themselves within a predetermined period of time by entering their network password. The time limit is set to tie the action of clicking on Accept and “signing” their action together. The default time is set to 20 seconds. Should the user not enter their password within the time period, then they will have to go back to the top of the policy, scroll down and click on Accept again.

It is for this reason that NETconsent recommends the security policy stipulates that users do not share password information and that this should be the first policy the user is required to accept.

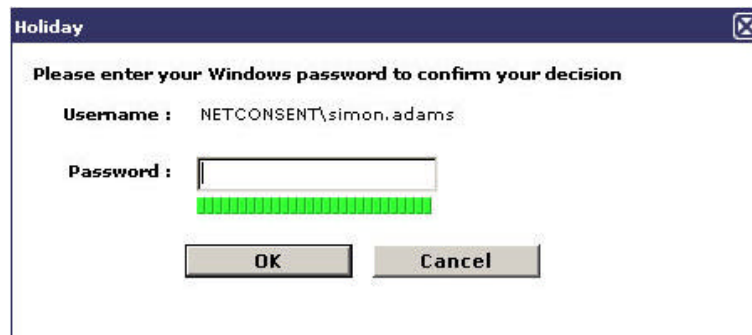


Diagram: User Authentication

If the user chooses to Decline a policy, they will be prompted to state a reason, which will be sent via email to the policy Administrator. It is recommended that you state the user is bound by the original policy until the dispute is resolved. For this reason the NETconsent solution still asks a user to authenticate themselves even if they choose to decline a policy. This action and any reasons are logged for auditing purposes.

Mandatory and Non Mandatory Policies

Policies are a written description of rights and responsibilities. They provide guidance for managers and others when deciding what to do in a particular circumstance. NETconsent splits policies into two types:

Mandatory

Key policies that should be accepted prior to users commencing activity.

Non Mandatory

Corporate policies which employees need to be aware of, but it is acceptable to introduce them over a period of time.

Mandatory Policy PEPs are typically used to deploy IT policies and restrict access to such IT services until a user has agreed to them.

The Information Commissioner states:

"The capabilities of electronic systems should be used to remind workers of their responsibilities. These can be set so that workers cannot proceed to access the internet or e-mail services without acknowledging the acceptance of certain conditions."

NETconsent supports the deployment of both Mandatory and Non-mandatory policies. NETconsent has developed PEP technology, with reference to legal, HR, compliance and audit requirements.

Mandatory Policy PEPs

- WEBconsent
- MAILconsent
- LANconsent

Non Mandatory PEPs

- LANconsent Pro

In many organisations, there are typically over 50 active policies at any one time. It is unrealistic for a user to have to accept all of these policies prior to being able to use network resources. Consideration should be given to the fact that:

- Employees will not digest and understand long or numerous policies
- Employees are there to work!

The majority of corporate policies will be stored against the LANconsent Pro PEP. LANconsent Pro enables organisations to schedule the rollout of policies over a realistic time period.

Recommended Implementation

To ensure users are aware of policies before they are potentially contravened, it is recommended that the following company policies be considered as Mandatory:

- **Security Policy**
- **Computer Workstation Usage Policy**
- **Health and Safety Policy**
- **Web Usage Policy**
- **E-mail usage Policy**

It is recommended that users are advised not to divulge sensitive information, such as passwords. NETconsent uses standard network IDs and Password to authenticate a user's acceptance of a policy. For this reason it is important that such information is kept confidential.

In a recent Employee Tribunal, a user argued that it was not he/she that accepted a specific policy. This notion was dismissed when evidence was produced that they had previously signed the security policy agreeing not to share password information. NETconsent's audit trail provided the necessary information and proof that the user had accepted the Security Policy and therefore the user had either breached this policy or that they had, in fact, read and accepted the subsequent policy. The court ruled in favour of the organisation.

It is recommended that some policies are disseminated over a period of time. An employee is unlikely to need to produce a holiday form within a few days of joining an organisation, therefore it would be wise to allow a reasonable period of grace before the policy requires acceptance. This allows users a sensible timeframe to read and digest numerous policies. Key policies, such as Disciplinary and Grievance procedures can be given a higher priority by assigning them with a lower Skip threshold. All Non-mandatory policies are listed in order of the Skip threshold set by the Policy Administrator, so at login users can immediately see which Non-Mandatory policies are waiting to be accepted. Users can decide to login and continue with their daily work until a more convenient time, unless the threshold limit has been reached, at which point the policy becomes mandatory and the user is required to agree to the policy prior to being able to login.

NETconsent recommends that policies are broken down into smaller, manageable documents. Experience demonstrates that the shorter the policy the more likely a user will read, understand and therefore abide by it.

Technical Deployment

NETconsent requires no client deployment as it runs via the browser. Therefore the NETconsent solution is extremely quick to deploy in an enterprise deployment scenario. The NETconsent Policy Server runs on Windows 2000/2003 servers running MS Internet Information Server.

WEBconsent integrates with MS ISA Server 2000/2004, Blue Coat SG Proxy Appliances, Net Cache Appliances, Squid Proxy and most other ICAP proxy servers.

MAILconsent integrates with Lotus Domino v5 and above and MS Exchange 2000 and above.

LANconsent integrates with MS Active Directory, NT4 networks and certain deployments of Novell networks (these require technical discussions with NETconsent technical staff).

All network traffic is via HTTP and HTTPS and network traffic is therefore minimal. The LANconsent Kiosk operates through a 50KB executable which is downloaded from the Domain Controller to the workstation PC if user activity to process Policies is required.

About NETconsent

NETconsent Ltd. is the world leading vendor of effective policy management and corporate communications software solutions. The NETconsent suite of products provides organisations with the ability to cost-effectively manage the deployment of corporate policies, user acceptance and access control to services. By automatically ensuring that users have the opportunity to read and accept (or reject) the current acceptable usage policy (AUP), prior to accessing a service, organisations are able to mitigate the risk of litigation and demonstrate compliance with corporate governance regulations. NETconsent solutions ensure that organisations can professionally manage users' acceptance of AUPs within a formal auditable legal framework whilst minimising the cost overhead.

For more information about NETconsent, visit www.netconsent.com

Disclaimer: This document is provided "as is" without any express or implied warranty. While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult a lawyer. The information provided here is for reference use only and does not constitute the rendering of legal, financial or other professional advice or recommendations by NETconsent Limited.