Dual ISP Bypass Proxy Feature Request

# Introduction

This Dual ISP Bypass Proxy Feature Request provides for a standard request form for schools to request local changes to their Dual ISP configuration. It is a document that aims to ensure that the school’s business requirements are met while maintaining alignment with the Department’s security policy.

The Department’s mandated Dual ISP solution provides a supplementary filtered Internet connection for all staff and students within the school. The *DECD ICT Security Policy* requires “*adequate audit logs, recording selected system activity and other security related events must be activated to assist in possible investigations and to allow access control monitoring. Log data must be appropriately protected, managed and retained*”.

Most risks introduced by bypassing proxy features are common to all schools considering this approach. To aid schools in understanding these risks, this document outlines these common risks. It is important to acknowledge that every school environment is different, and it is the Principal’s responsibility to review these risks and consider their environment for any additional risks that may be present.

## Bypass Proxy Authentication

To fulfil the *DECD ICT Security Policy* requirement, the Dual ISP solution necessitates that all users of the supplementary Dual ISP Internet connection must authenticate with valid account details from the school’s local Active Directory. When supported client devices are connected to the local school’s Active Directory this authentication process is transparent to the user and generally provides a seamless user experience.

There are some scenarios where the client devices may not authenticate automatically or may not support proxy authentication. For devices that do not support proxy authentication, the school can request that authentication to be disabled on a per device (client IP) basis. Another scenario is where a specific application requires access to the Internet and does not support proxy authentication. The school may also request authentication be disabled on a per URL (website) or server IP address basis.

Bypassing authentication at a local school level requires careful consideration. Bypassing authentication creates additional risks that the authentication process normally manages and minimises. Locally the school will need to ensure steps are taken to manage and minimise all identified risks to an acceptable level.

## SSL Content Inspection Whitelisting

The Dual ISP solution supports SSL content scanning and inspection - including certificate verification, applying antivirus scanning and web filtering to the encrypted traffic. There are some scenarios where the client devices and/or software are unable to communicate with the destination URL (website) with content inspection enabled.

Content inspection whitelisting for URL’s at a local school level requires careful consideration and creates additional risks that the inspection process normally manages and minimises. Locally the school will need to ensure steps are taken to manage and minimise all identified risks to an acceptable level.

## Full Bypass Proxy by URL or IP Range

Bypassing all authentication, content scanning, inspection and web filtering at a school level requires careful consideration. This option is only available if all other troubleshooting options have been explored, with assistance from DECD ICT Services.

Locally the school will need to ensure steps are taken to manage and minimise all identified risks to an acceptable level.

# Procedure

The following steps outline the process required to submit the request. Sites must complete Part 1, Part 2 and Part 3 of this form prior to submission.

## Process Steps

### The Authorised Site Representative should work together with the staff at the site to complete Part 1, Part 2 and Part 3 of the request form. Additional guidance on completing the form may be obtained through the ICT Service Desk.

### It is necessary to obtain signoff from the appropriate Principal or Director. Once signed, scan and email this form to the DECD ICT Service Desk - [ictsupport@sa.gov.au](mailto:ictsupport@sa.gov.au) or fax to the ICT Service Desk on (08) 8410 2863. A copy of the signed request must also be maintained at the requesting school.

### Once the request has been received by the ICT Service Desk it will be forwarded to the ICT Assurance team for further assessment and review.

### Where there is no significant impact to department/school information assets identified, the change will be approved to be made to the local Dual ISP configuration for the school.

### Where the assessment determines that there is potential for significant impact to department/school information assets, further discussion and consultation will be undertaken by ICT Assurance direct with the school to obtain signoff or alternatively to modify the request/impacts.

### Once the assessment has been approved, timing of the change will be scheduled with the local site technical staff. The site will be responsible for providing advanced notification to its affected users.

### Infrastructure Support Services will provide the technical support model. The local technical staff at the school will be the contact point for all user queries at the time the change is applied.

### Sites are advised to ensure that any new Principal to the site reviews the assessment to ensure the risks are understood. The Department’s ICT Services should be contacted if any changes are required.

# References and Definitions

The following department ICT security documents are relevant and should be read in conjunction with this procedure:

* DECD Policy – ICT Security  
  <http://www.decd.sa.gov.au/docs/documents/1/DECD_Policy_ICT_Security.pdf>
* DECD Policy - Internet Access and Use  
  <http://www.decd.sa.gov.au/docs/documents/1/DecdPolicyInternetAccessa.pdf>
* DECD Standard – School ICT Network Security  
  <http://www.decd.sa.gov.au/docs/files/communities/docman/1/DECS_Standard__School_ICT.pdf>

Part 1 – Technical Change Details

Complete the following table which gives background information about your requested change. The detail given in this table will provide a basis for the thinking required in the risk assessment table that follows in Part 2:

|  |  |
| --- | --- |
| **NOTE: To avoid delay please ensure all parts of this form, including authorisation, are complete before faxing to (08) 8410 2863 or emailing a scanned copy to ictsupport@sa.gov.au.** | |
| **REQUESTOR DETAILS – Complete all sections** | |
| Surname: | Given Names: |
| Position: | Phone Number: |
| E-mail address: | Employee ID/Contractor ID: |
| Location Name: | Location Number: |
|  |  |
| **REQUEST TYPE** | |
| BYPASS PROXY AUTHENTICATION  SSL CONTENT INSPECTION WHITELISTING  FULL BYPASS PROXY BY URL or IP range | |
| **BUSINESS AND TECHNICAL REQUIREMENTS**  (*Provide details as to why this change needs to be implemented and the changes required)* | |
| GoToWebinar is a product provided by Citrix for providing Video and Audio Conferencing solutions via the Internet.  GoToWebinar uses HTTP/HTTPS outbound connections to transparently enable screen-sharing sessions, but does not work with the Dual ISP MWG solution due to SSL Inspection.  The following URLs are required to entered into the SSL Inspection Bypass List:  regex(([\w.-]\*\.|\.?)gotowebinar\.com(\/.\*|\/?))  regex(([\w.-]\*\.|\.?)citrixonline\.com(\/.\*|\/?)) | |
| Implementation Timeframe  *(Advise of proposed time frame for change to be implemented)* | |
| ASAP | |
| Access Timeframe | |
| Is the access required permanent or temporary**?**  PermananeNt  temporary  If temporary, what is planned end date of the required access?  date **XX/XX/XXXX** | |

Part 2 - Risk Assessment for Dual ISP – Bypass Proxy Feature

In understanding and assessing the level of risk that exists in relation to Department information assets, school management needs to consider the potential impact should any identified risks arise, as well as the likelihood of such an event. This will provide the basis for the overall assessment of the level of risk that is faced. The process and documentation outlined in this section is required under the SA Government’s mandated Information Security Management Framework (ISMF).

Most risks introduced by bypassing features are common to all schools considering this approach. To aid schools in understanding these risks, this document outlines these common risks. It is important to acknowledge that every school environment is different, and it is the Principal’s responsibility to review these risks and consider their environment for any additional risks that may be present. In assessing the Consequence, Likelihood and Overall Risk rating, the site should follow the Risk Ratings within the matrix in Appendix A.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RISK DESCRIPTION** | **SUMMARY OF RISK MANAGEMENT PRACTICES (CONTROLS) ALREADY IMPLEMENTED** | **CONSEQUENCE**  **(1—5)** | **LIKELIHOOD**  **(1—5)** | **OVERALL RISK RATING** | **RISK TREATMENT**  **Further actions required to monitor risk or improve controls, or comment on acceptance of risk.**  ***These actions will contribute to minimising identified risks*** |
| Activity associated with client devices cannot be attributed to the exact individual user at the time of client asset use. | The McAfee Web Gateway solution provides for the logging of IP addresses and the web activity. Reports can be produced that can attribute activity to an IP address. | 3 | 5 | H | This risk is inherent to the bypass request. Technical controls the site could possibly implement that will assist in associating the activity to a device and/or user include;   * Retain DHCP logs (when combined with the available reporting) * Register of Device/MAC Address and allocated user/owner (when combined with the available reporting) * Force static based IP addresses on MAC address * Implement an alternative form of authentication that integrates with the school network |
| Access to inappropriate content by users when accessing the Internet on devices in bypass list. | ICT Assurance release communications to assist site leaders to evaluate and review access rights and risk minimisation strategies that provide confidence that policy and procedures are understood and complied with to assure ongoing improvement in this area.  ICT Assurance communicate with site leaders reminding them of other obligations that preschools directors and school principals are responsible for ensuring that each education site has a process in place for ensuring students are not placed at risk when accessing the Internet.  All users are required to read, acknowledge and sign the DECD Standard - Acceptable Use Policies for Schools, Preschools and Children’s  Services Sites | 3 | 3 | M | * School to ensure user acceptance policy is signed-off by student/parent/guardian. * Client assets that are configured in the bypass list are generally used by students when under staff supervision. Staff will need to ensure that this is adhered to. |
| Bypass form assessment process delays school implementation timeframe. | The evaluation process is clearly documented and agreed upon by all teams.  Clear escalation points are available for all parties involved. | 3 | 2 | M | * ICT Services will continue to review their operational processes. * ICT Assurance holds weekly service delivery meetings at which time open/outstanding requests are reviewed. |
| Access to inappropriate material may be delivered via the sites listed in the SSL inspection Whitelist |  |  |  |  | * Site is to use GoToWebinar for delivering content to specific users * Not to be used for any remote connections/support to a device within the school network |
| *These rows are intentionally left blank for the insertion of site specific risks, controls and treatments identified during the risk assessment process* |  |  |  |  |  |
| *These rows are intentionally left blank for the insertion of site specific risks, controls and treatments identified during the risk assessment process* |  |  |  |  |  |

Part 3 – Acceptance and Authorisation

Once the Risk Assessment in Part 2 is complete, the following authorisation and acceptance of identified risks needs to be completed prior to submitting Part 1, Part 2 and Part 3 to the ICT Service Desk for processing. This can be done by faxing to ICT Service Desk on (08) 8410 2863 or by scanning and emailing to [ictsupport@sa.gov.au](mailto:ictsupport@sa.gov.au). The request will be reviewed by the Manager, ICT Assurance before final approval.

In signing this, you acknowledge that you have understood and assess the risks provided, along with the sites own Risk Assessment during this process.

|  |  |
| --- | --- |
| Applicant’s Authorisation | |
| **Applicant’s Name** |  |
| **Applicant’s Signature** |  |
| Principal / Director Authorisation & Acceptance | |
|  | |
| **Principal’s / Director’s Name** |  |
| **Signature** |  |
| **Phone Number** |  |
| **Email Address** |  |
| **Date** |  |
| In authorising this request, I confirm in relation to the Bypass of Proxy Authentication in the Dual ISP solution that I have read and understood the requirements of the:   * DECD Policy – ICT Security[[1]](#footnote-1); and * Information Security Management Framework [ISMF][[2]](#footnote-2)   I acknowledge that it is the responsibility of the school to ensure:   * All Students and Staff are educated in the appropriate usage of the system; and * Effective risk treatment procedures are in place as outlined within this request. | |

Appendix A: Risk Ratings Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Consequence** | 5  Critical  Ongoing loss of critical infrastructure and systems | M | H | H | E | E |
| 4  Major  Major disruption of business | M | M | H | H | E |
| 3  Moderate  Moderate disruption of business | L | M | M | H | H |
| 2  Minor  Minor disruption of business | L | L | M | M | M |
| 1  Insignificant  Negligible impact on customer base. | L | L | L | M | M |
|  | 1  Rare  Possibility of occurrence less than 5% | 2  Unlikely  Possibility of occurrence between 5% - 25% | 3  Possible  Possibility of occurrence between 25% - 50% | 4  Likely  Possibility of occurrence between 50% - 75% | 5  Almost Certain  Possibility of occurrence more than 75% |
| KEY  L = Low M = Moderate H = High E = Extreme | | **Likelihood** | | | | |

|  |  |
| --- | --- |
|  | Low |
|  | Moderate |
|  | High |
|  | Extreme |

For further information refer to the DECD Procedure – ICT Security Risk Assessment – <http://www.decd.sa.gov.au/docs/documents/1/DecdProcedureIctSecurityR.pdf>

1. DECD Policy – ICT Security - <http://www.decd.sa.gov.au/docs/documents/1/DECS_Policy__ICT_Security.pdf> [↑](#footnote-ref-1)
2. Information Security Management Framework [ISMF] - <http://www.dpc.sa.gov.au/sites/default/files/pubimages/documents/ocio/ISMF_v3.pdf> [↑](#footnote-ref-2)