

Credential / Key Application Form & Notes

The *Credential / Key Application Form* affords a long-term means of access to one or more Telstra network sites. This will generally be via an Electronic Access Control System (EACS) card or physical key in both metropolitan and country areas.

Should your need be for temporary or short term access, Security Access Management at Network services may be able to assist you in arranging a loan key or EACS access.

Instructions for Completing Credential / Key Application Forms

The application may be completed in handwritten or in **bold type**, and forward it to the appropriate **Responsible Manager** (refer **Responsible Manager Details** below), who must endorse the request, including the mandatory requirement that the appropriate induction training has been completed. Once completed e-mail the completed signed application to Telstra Wholesale for processing.

Further instructions on how to complete the application form are set out below.

Type of Application

You must nominate the type of application being made (i.e. "New", "Change of Access", "Change of Details", "Temporary" or "Replacement" of a lost, faulty or damaged EACS card or key).

Faulty or damaged cards or keys should be returned to the specified postal address, as provided in the Contact Details section of this document (ordinary mail acceptable). Please phone Telstra wholesale or Security Management Centre before returning faulty or damaged cards so that the EACS cards can be disabled.

Notes: Lost cards or keys pose a security risk. You are expected to be responsible for the safe carriage of them at all times. Under no circumstances should the cards or keys be marked or carried with other items that may help others identify their purpose. For example, do not keep the credential/card on a chain together with your ID card! Lost or misplaced cards should be reported to Telstra Wholesale immediately, at which time the card will be disabled rendering it unusable.

Applicant's Details

You must supply personal details as required in the form. Your first name should be your full legal name, not preferred name, unless all your other personal records reflect this. If you have been provided with a Telstra ID card, please quote the employee number on the back of the card. For all EACS card applications, other than "New" applications, please quote your existing EACS card ID number, which is normally a 7 digit (sometimes a 9 digit) number stamped on one side of the card. EACS cards can be programmed or re-programmed for use in all states and territories

Note: All staff whether they had a Telstra ID or not, **MUST** complete the Skilled course.

<http://www.telstranetworkinduction-physicalsecurity.com.au/>

Access Required

You must nominate the specific sites or region of sites for which you require access. For broad access to all sites, a detailed business justification will be required. For both EACS card and key access, you must specify the days of the week, hours of the day and dates for which access is required. For **Change of Access** requests to electronic card/keys, all existing and proposed new sites need to be stated, otherwise all previous access may be deleted. In the case of mechanical key access, please specify key types and key numbers (which are normally embossed and/or stamped on the side of the key). **Note** If access to a large number of sites is required, you should list those sites on a spreadsheet and attach the spreadsheet to the application form.

For contractors, an end of contract expiry date should be provided (maximum 3 years). An option is to match EACS with the HR End Date. If an End Date isn't provided then a default of twelve months will be entered in EACS.

Contractor's Representative/Additional Endorsement/Responsible Manager Details

For all Carriers/network providers, Carrier contractors and sub-contractors, supply details of the person delegated as the **Contractor's Representative / Additional Endorsement**

In general terms, sign-off by the Carrier / Carriers representative (authorised contractor) provides confirmation that the applicant has legitimate operational purpose for requiring the stated access, as per the Business Justification stated in the application form, and will ensure that the applicant has received appropriate induction training (a Health & Safety requirement). A check-box is provided to indicate this. Responsible manager authorisation is Wholesale Facilities Access.

Miscellaneous

Requests for access to network CBD on-site car parks require additional approval from the relevant Facility Manager, whose contact details are available from the Security Access Management Team at Physical Access & Security

IDC restricted areas have additional access requirements which are available upon request from Telstra Wholesale.

EACS System / Using an EACS Credential

- The credential is a cream /grey card of credit card proportions with no identifying markings other than a number. The door readers are similarly unobtrusive – grey box with 3 LEDs or more commonly used black box with one tri-state LED. An amber LED indicates a system normal condition.
- When a card is passed in the vicinity of a card reader, the response will either be a change of LED colour from amber to green and release of the door lock (refer next item), or amber to red indicating that your card is not programmed for access to that reader or site, or if there is no change of LED colour, your card may be faulty, requiring replacement.
- If the Last Man Out (LMO) feature is installed and functioning in a building, the first pass of the card will not release the door lock, however the intruder alarm points/perimeter doors will have been disabled. A **second** card pass will unlock the door to allow entry.
- If you are the last person to leave the building, all intruder alarm points/perimeter doors and EACS doors need to be set/closed, and the LMO button pressed. A high pitched tone will sound for between 10 and 30 seconds to indicate the LMO function has been successfully activated, and you may now exit the building. There should be a notice inside the door providing further information on this subject.

Contact Details for Telstra Wholesale

Facilities access:

twsiteaccess@telstrawholesale.com

<https://www.telstrawholesale.com.au/products/facilities.html>

<p>All States & Territories</p> <p>All Carriers / Network Providers</p> <p>and</p> <p>All Shared Facilities Users</p>	<p>Physical and Postal Address:</p> <p><i>Telstra Wholesale</i></p> <p>23rd Floor, Argus Centre 300 Latrobe Street, Melbourne. VIC 3000.</p> <p>Ph. 03 8649 7591</p> <p>Locked bag 5686 Melbourne, Vic. 3001</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Code of Conduct

Responsibilities for Network Site Entry

GAINING ENTRY

1. Access to sites is only for legitimate business purposes.
2. Provide appropriate notice per "Attendance Request Form" for carriers or shared facility users.:
https://www.telstrawholesale.com.au/content/dam/tw/products/Facilities%20Access/TEBA/Documents/Order_forms/credential-key-application-form.docx
3. Attending Non-EACS sites – Complete a once off registration with Network Services, Special Services Team on 1300 652 235 option 2, 5, 1. Then when attending Non-EACS sites, register your site attendance via a phone call or SMS to 0427 767 462 supplying the Node Code and expected duration (an SMS is preferred). Further information is available from "Attendance Notification at Network Sites"
4. Take all necessary action to be informed about personal conduct and site safety (including potential Occupation Health and Safety risks).

STANDING SECURITY INSTRUCTIONS

1. Ensure that all external and internal site and building entry doors and gates are kept closed and locked at all times.
2. Challenge & disallow entry to "tail-gators" refer them to their manager/contract manager to arrange authorise entry.
3. Immediately upon arrival at a site requiring a physical key for access, record your attendance in the site log.
4. Comply with "Last Man Out" Site Poster – Building security / LMO Button
5. All security incidents must be reported promptly, via the Telstra Security Incident Reporting (SIR) process or to the Telstra Wholesale Facilities Access.

OBLIGATIONS AND CONDUCT

1. It is the responsibility of all staff on Telstra sites to work safely, protect others from possible hazards and abide by all Occupation Health and Safety guidelines, NO SMOKING policy is to be observed in all Telstra buildings.
2. Wearing of a Telstra identification pass is mandatory in all Telstra buildings and sites, **except where one is not issued, an alternative means of photo identification (such as a driver's license or company ID card) and approved ARF "Attendance Request Form": must be carried and produced if requested by Telstra or an authorised representative.** No mobile phones, two-way radios or cameras are to be used in any equipment room. These devices can cause network outages that could lead to your organisation incurring service restoration costs.
3. Sites should be left clean and tidy, and all rubbish removed.
4. Access to sites, including any external or internal electronic controlled doors and gates, must always be made using a credential / key that has been issued to the person requiring access.
5. Personal use of on-site Telstra equipment (including telephones) is prohibited, except when approval has been granted.
6. Any information obtained whilst on Telstra premises must be regarded as strictly confidential and falls under the Privacy Act.
7. Report all door faults to the National Thies Fault Centre on 1300 363 869 opt 1

USE OF CREDENTIAL / KEY

1. Do not mark or otherwise attach the credential / key with any identifiable item such as an ID card.
2. Do not leave the credential / key in an unattended or unsecured place, such as in an unattended vehicle, particularly overnight, even when parked in a seemingly secure location.
3. **Do not loan the credential / key to anybody, as it is not transferable.** The recipient of the credential / key is responsible for use and security, and shall immediately report any loss or misuse to **Telstra Wholesale** 03 8649 7591 or Security Access Management on 1300 363 421, option 1.
4. As the credential / key remains the property of Telstra, if no longer required, or is faulty, please return it to **Telstra Wholesale** or Security Access Management Centre, who should be contacted on 1300 363 421, option 1 during business hours to discuss the process involved.
5. **Management reserves the right to revoke access at any time, with or without prior notification.**

COMPLETE THE FOLLOWING APPLICATION FORM

Email application to twsiteaccess@telstrawholesale.com

CREDENTIAL / KEY APPLICATION FORMwebsiteaccess@telstrawholesale.com - Ph. 03 8649 7591

Place an 'X' in one box only	Place an 'X' in appropriate box(s)		
Device Type <input type="checkbox"/> EACS CARD <input type="checkbox"/> PHYSICAL KEY NOTE: Separate applications required for <u>multiple</u> Device Types.	<input type="checkbox"/> New <input type="checkbox"/> Change of Access (Refer Access Required - above) <input type="checkbox"/> Change Details: Card Holder <input type="checkbox"/> Company Name <input type="checkbox"/> Contact Details <input type="checkbox"/> <input type="checkbox"/> Replacement: Lost <input type="checkbox"/> : Faulty <input type="checkbox"/> Damaged <input type="checkbox"/> (Please return)		
Applicant's Details (Name of Card / Key Holder)			
Existing Card / Key Number		Company Name	
Replacement Card / Key Number		Address	
Full name		Office Phone	
DOB		Mobile	
Telstra Site Induction Ref	SKA	E-Mail	
Access Required			
Note: For access to any requested restricted sites (floors & CBD car parks) additional approval must be gained prior to access.			
<u>State</u>	<u>Name of Sites / Region / Building Floors</u>		
<u>Business justification:</u>			
Code of Conduct acceptance			
Please confirm the following <input type="checkbox"/>			
<p>I understand that access privileges provided as a result of this application are subject to terms and conditions of the Code of Conduct governing access to Telstra Network Facilities and that I am accountable for EACs cards and keys issued to me as well as any loss or damage incurred as a result of their use until returned.</p> <p>As I am making this declaration on behalf of others, I accept full responsibility for ensuring that the ultimate EACs/key holder will be made aware of and agree to abide by those terms and conditions as set out in the Code of Conduct prior to being issued with card/key and that they acknowledge the obligation to maintain the security of Telstra's network facilities at all times in compliance with the below standing security instructions as set out below, and in the Code of Conduct.</p>			
Standing Security Instructions.			
<ol style="list-style-type: none"> 1. Ensure that all external and internal site and building entry doors and gates are kept closed and locked at all times. 2. Challenge and disallow entry to "tail gators" and refer them to their Manager/Telstra Wholesale to arrange authorised entry. 3. Immediately upon arrival at site requiring a physical key for access, record their presence in the site log. 4. Comply with the "last man out" Site poster and - building security /LMO button process. 5. Ensure <u>all security incidents</u> are reported promptly to Telstra Wholesale facilities access 			
Identity & Access Services may disable and recover access cards/keys at any time for noncompliance with this agreement. Please note there may be a once off charge for Lost EACS cards or Keys.			
Carrier Signoff			
To be endorsed by either a carrier representative or an authorised contractor.			
	Name		
	Job Title		
	Mobile		
	Email		
	Signature		
	Carrier		
	Name and address for dispatch		