

Section A – Which level do I use?

NATS Unclassified

This guide provides a framework which allows the business to share information confidently knowing it is reliable and protected to an agreed standard.

Follow 'The Process' to start with and this will refer you to other supporting information within this guide.

<p>LEVEL 1 NATS Unclassified</p> <p>Information which if disclosed, either intentionally or unintentionally, to an external person or organisation would cause no damage or embarrassment to personnel or NATS.</p>	<p>LEVEL 2 NATS Private</p> <p>Information that NATS needs to process and share to deliver services and conduct administrative/HR functions.</p> <p>The unauthorised disclosure of this information, even within the company, could cause significant harm to the interests or reputation of NATS or its people. This would normally have an effect of financial loss, loss of business opportunity, embarrassment or loss of brand reputation. Such information may include, but is not limited to:</p> <ul style="list-style-type: none"> negotiating positions marketing information competitor assessments personal information (Data Protection Act 1998) customer information development and operation of policy commercial contracts business continuity and crisis management plans. 	<p>LEVEL 3 NATS Protected</p> <p>The unauthorised disclosure of this information, even within the company, could cause serious damage to the interests of NATS or its people. It could result in serious financial loss, severe loss of business opportunity, grave embarrassment or long term loss of brand reputation. Such information may include, but not limited to:</p> <ul style="list-style-type: none"> details of major business plans, acquisitions, mergers sensitive competitor, partner or contract assessments sensitive operational data sensitive security information large volumes of Personal Information (Data Protection Act 1998).
--	--	--

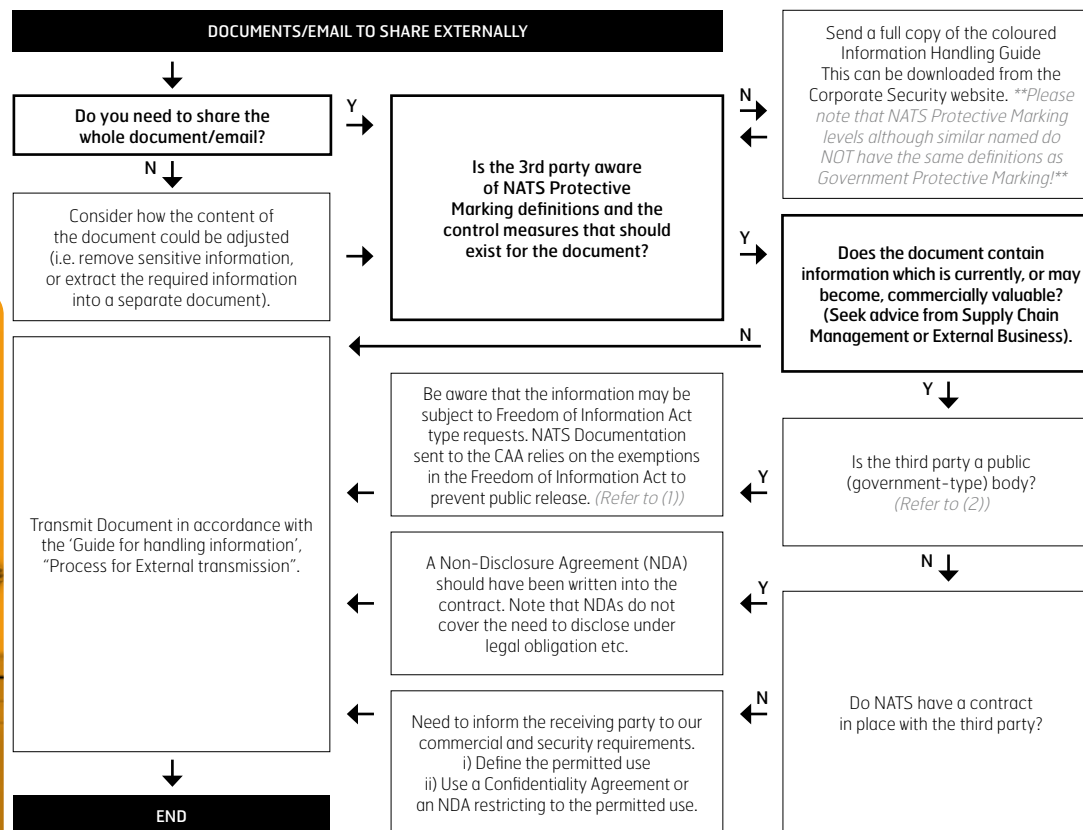
This guide has been produced in line with NATS Protective Marking Policy. The policy and more details regarding Information Security can be found in the Security Manual, Chapter 4, Leaflet 5, or contact:

NATS Corporate Security
01489 612125

24/7 Out of Hours
01489 612364

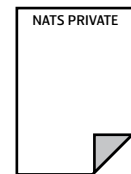


Section C – Sending information externally

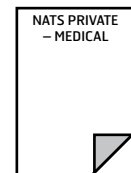


- (1) Current agreement with the CAA – there is information that NATS is required to share with the CAA. A provision is in place to protect certain information from disclosure for more information on this please refer to article 18 of the Regulation 550/2004 (Service Provision Regulation). Also refer to (2) below when sharing information with CAA.
- (2) Extra care must be taken when sharing information with Government/Public Bodies (they are subject to Freedom of Information Act 2000 (FOI). In order to begin to meet the requirements for exemption under FOI, information/documents MUST have the appropriate Protective Marking.

should be either NATS UNCLASSIFIED or NATS PRIVATE. Very little information generated within NATS will come under NATS PROTECTED.



3 Apply Protective Marking and Descriptor Suffix (this is optional).



4 What do you want to do with document now?

Internal: Refer to **Section B**.
External: If you are going to share the information externally then refer to **Section B and C**.

The Process

- 1 Create document.
- 2 Apply appropriate Protective Marking. Refer to **Section A**.
All paper-based or electronic information created should have a header printed on each page stating the Protective Marking. In general, most of your documents and data

NATS Unclassified
Protective Marking Guide

Create it,
Label it,
Protect it!



Section B – Guide for handling information

TYPE	PROCESS			
	Labelling	LEVEL 1 NATS Unclassified	LEVEL 2 NATS Private	LEVEL 3 NATS Protected
Electronic information (incl. email)	General protective measures	Consider converting to PDF to ensure integrity of the document.	<ul style="list-style-type: none"> May only process information via NATS configured IT services Extra care must be taken when processing information within a public area i.e. internet cafe, train or anywhere people can look over your shoulder Review access privileges to electronic storage area regularly e.g. LiveLink Only print if really needed Removable media (USB, CDs) – must be password protected. 	As NATS PRIVATE plus: <ul style="list-style-type: none"> Must be password protected for storage Do not print without consent from the originator.
	Internal transmission	No restriction.	<ul style="list-style-type: none"> Can be sent within NATS but the author/creator may choose to limit distribution. 	<ul style="list-style-type: none"> Must be password protected for transmission Identify and double check distribution list before sending.
	External transmission	<ul style="list-style-type: none"> No unauthorised distribution Ensure 'Security Statement' appears within the document. This can be found in the NATS Protective Marking Policy in the Security Manual, Chapter 4, Leaflet 5. 	As for NATS UNCLASSIFIED <ul style="list-style-type: none"> Refer to 'Section C – Sending Information Externally Process'. 	As NATS PRIVATE plus: <ul style="list-style-type: none"> All email or electronic transmission to be encrypted. (Contact IS for advice on encryption or visit the IS website) Email to CAA addresses is automatically secured Must be encrypted if stored or transported on CD, DVD, memory sticks or other portable media.
	Disposal	<ul style="list-style-type: none"> Media (e.g. hard drives, USB, CDs etc.) is to be destroyed in accordance with NATS policy as detailed in the NATS Security Manual Delete information when no longer required in accordance with NATS Information Lifecycle Policy. 	As for NATS UNCLASSIFIED.	As for NATS UNCLASSIFIED plus: <ul style="list-style-type: none"> Delete mail from folder when no longer required.
Paper information	General protective measures incl. photocopying	No restriction – although clear desk policy does apply in NATS.	<ul style="list-style-type: none"> Do not leave unattended on desk, even for short periods of time Information must be locked away when not in use and secured at the end of the working day No restriction on photocopying on NATS premises. 	As NATS PRIVATE plus: <ul style="list-style-type: none"> Information must be stored in a suitable lockable cabinet and keys must be controlled Do not remove paper copies from the work place unless absolutely necessary Photocopying is not recommended unless absolutely necessary and then must be authorised by author creator.
	Internal circulation	No restriction – transit envelope will suffice.	Single sealed envelope with no Protective Marking. Addressed specifically for the attention of the named individual and marked 'Personal for'.	As NATS PRIVATE <ul style="list-style-type: none"> Put into a sealed envelope, sign over seal and marked NATS PROTECTED. The envelope should then be placed into another envelope which should be addressed but DO NOT mark with Protective Marking or content.
	External circulation	<ul style="list-style-type: none"> No restriction – single sealed envelope with no marking No unauthorised distribution. 	As for internal circulation plus: <ul style="list-style-type: none"> Ensure 'Security Statement' appears within the document Refer to 'Section C – Sending Information Externally Process'. 	Not recommended but if necessary put into a sealed envelope, sign over seal and marked NATS PROTECTED. The envelope should then be placed into another envelope which should be addressed but DO NOT mark with Protective Marking or content. It should then be sent Recorded or Registered delivery and sender must retain proof of postage. Or use a trusted person to hand deliver.
	Disposal	No restriction – advise to follow best practice as NATS PRIVATE.	Shredded using a cross cut shredder or placed in confidential waste sacks.	As NATS PRIVATE.
Fax	Internal/External transmission	No restriction.	<ul style="list-style-type: none"> No restriction from NATS premises Must telephone ahead to make sure the recipient is aware the fax is going to be sent. 	NOT permitted unless absolutely necessary.

NOTE: All of the above recommendations are to be used in conjunction with NATS Acceptable Use Policy.