

Instructions

1. Follow State security policy in [Information Technology Security Policy- Contractor 230.77](#), (ITSP- Contractor) the policy can also be found at bit.sd.gov/vendor/default.aspx.
2. Fill out the required section of this form and obtain approvals.
3. Send the completed certificate to the State Contact.

Section 1. Required

Requestor Name Company Email Phone Classification of the confidentiality of the data	[Person filling out this form, requesting the sanitization] [Example- Moderate, see ITSP- Contractor 230.77, Data Classification Table can be found on the Vendor Information webpage.]
Data Owner State Contact	[The State agency that is the data owner Current State agency contact]
Person conducting the sanitization Company Email Phone	
Database Name	
Type of media Model Serial Number	[For example- Hard Drive HPE model # 512547-B21 12345]
If there are copies of the data, list the location	
Type of sanitization Method used to sanitize Tool used to sanitize	[For example- Purged Microsoft SQL Server purge function Microsoft SQL Server 2014]
Was the data one of the following:	<input type="checkbox"/> FTI <input type="checkbox"/> ePHI <input type="checkbox"/> FPLS <input type="checkbox"/> CJIS
Person who verified the sanitization Date Email Phone	[This person should be different then the person doing the sanitization.]
Verification Method	
Verification Notes	
If the media was reused what are the destination details	[Example- Media was reused by (name) data center. Note only data that is classified low or moderate confidentiality can be reused, see ITSP- Contractor 230.77.]

Section 2. Approvers

Approvers	Signature	Date
[Name of Sanitizer]		
[Name of Verifier]		
Wayne Hayden-Moreland Data Center Director		

This certificate must be sent to the State Contact who will send it to the Data Center Director. Electronic copies are acceptable.