Risk Assessment Number	14
Dataset	Secondary Substation
No. Data Tables	4
Date	November 2024
Refresh Date	November 2025
Approver	Kirsty Scott

1. Principles

SPEN classify their data into three categories, based on the risk assessment outcome:

- *Open*: data is published for all to use, modify, and distribute with no restrictions.
- *Shared*: data is published to a limited group of participants with restrictions on usage.
- *Closed*: due to sensitivities within the data, it is not suitable for publication, however, may be shared with specific stakeholders under a bespoke data sharing agreement where appropriate.

The risk assessment determines the classification and whether it can be published.

The risk assessment considers 6 categories:

1. *Personal privacy*
2. *Security*
3. *Public interest*
4. *Commercial*
5. *Legislation/Regulation preventions*
6. *Other*

Risk scoring is based on a combination of the likelihood of the risk occurring and the impact of it – with an outcome between 0 and 10.

- Risk score of 4 or below: no mitigations applied.
- Risk score of 5-7: mitigations required to be applied before publication.
- Risk score of 8 or above: due to sensitivities within the data, dataset may be categorised as 'Closed' and not suitable for publication.
- If the **total** risk score after mitigation is above an 8 then the dataset is classified as 'Closed' and not suitable for publication.

The mitigations that can be applied are as below:

1. *Aggregation*: combining/summarising in order to reduce granularity whilst still maintaining some value.
2. *Anonymisation*: removal/partial removal of identifying features, e.g. location info, name, address, postcode.
3. *Delay*: deferring release of data for a defined period until a time where the risk is greatly diminished or no longer exists, e.g. outage data could be used to target the network when some sections are placed under greater load, therefore a delay in publication could be implemented to mitigate the risk of the data being used to attack the network.
4. *Pseudonymisation*: replacing identifying features with a different unique identifier, e.g. replacing name and address with an ID that is held internally.
5. *Redaction*: removal or overwriting of features.
6. *Restrict use and access*: e.g. subject to shared data licence conditions, user registration and approval.
7. *Other*: any other mitigating action that could be applied, details of the action are provided in the risk assessment.

Name of Dataset:	Secondary Substation Data	
Date of Assessment:	01/11/2024	
Dataset Owner:		
Assessment completed by:		
Dataset Description:	SPEN Secondary Transformer Rating SPEN Secondary Transformer Expected Utilisation SPEN Secondary Substation Customers Connected SPEN Secondary Substation Upstream Primary Substation	
When assessing below, for all sections, consideration must also be given to other datasets that may be openly available elsewhere (within or outwith the organisation) that when combined with this dataset could create sensitivity issues. Do not consider in isolation.		
Risk Assessment: **If issues exist, mitigating actions must be listed within the Risk Scoring and Mitigation Table - see overleaf**	PERSONAL PRIVACY: Is personal data contained in the dataset pre-mitigation? Considerations: 'Personal Data' means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly by combining with other information, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Public information can still be personal information, e.g. a satellite image of a house may be personal information that relates to an individual.	YES
	SECURITY: Does the dataset, pre-mitigation, include factors that would change the security posture of individuals, entities or impact national security? Considerations: If the dataset contains personal data, would publication of that data go against the rights and freedoms of the individual. If the dataset contains confidential business sensitive information (such as financial information or physical asset information), would publication of that data go against the obligation to implementation appropriate technical and organisational measures to protect that information. If the dataset contains details of physical locations or structures, would the publication of that data go against the requirements to protect staff, the public or company infrastructure.	YES
	PUBLIC INTEREST: Does the dataset, pre-mitigation, have the potential to negatively impact public interest? Considerations: Could the dataset be reasonably interpreted, intentionally or unintentionally, in a way that would be detrimental to the public good or what is in the best interest of society. Does the data allow for good decision making by its users that allows for an efficient allocation of resources to meet overall stakeholder aims. Could the dataset be used in a way to restrict fair commercial competition. Does the dataset have appropriate transparency and accountability assigned to provide users comfort over the quality of data and its intent.	YES
	COMMERCIAL INTEREST: Does the dataset, pre-mitigation, contain information that through its disclosure would, or would be likely to, prejudice or harm the commercial interests of SPEN, those of an individual or customer, a company or another legal entity? Considerations: Are there intellectual property restrictions whereby the data has been obtained by SPEN but with terms and conditions imposed which would restrict onward publishing.	YES
	LEGAL / REGULATORY OBLIGATIONS: Does the dataset, pre-mitigation, breach any law or regulations to which SPEN is subject? Considerations: Are there specific legislation or regulation that prohibits publications in whole or in part? These laws include, but are not limited to: Utilities Act 2000; Electricity Act 1989; Gas Act 1986 / 1995; Competition Act 1998; Enterprise Act 2002; Enterprise and Regulatory; Reform Act 2013; Data Protection Act 2018; General Data Protection Regulation (GDPR), Network and Information Systems Regulations 2018	NO
	OTHER: Other personal privacy, security, public interest, end consumer, legislation/regulation risk, health and safety implication risk? For example risk of health and safety being compromised? Is data quality substantially poor and substantially inadequate at meeting users needs?	YES

Classification	Published under a Shared Data Licence

Ref	Sensitivity Area	Risk Details:	Risk Impact before Mitigation	Risk Likelihood before Mitigation	Risk Score	Mitigating Actions	Risk Impact after Mitigation	Risk Likelihood after Mitigation	Risk Score	Action Taken / Comments
1	Personal Privacy	If there is a mistake in the records of customer numbers, it is possible that maximum demand usage data is shared for four or fewer customers. Less information can be inferred from MDI data than it can from detailed load profile data. Therefore it is assumed that the GDPR-associated impact is less severe.	Significant	Possible	6	Redaction	Significant	Remote	4	Identify the data owner for the number of customers connected at each secondary substation, and confirm that the records are reliable for the redaction of GDPR-sensitive data (customer numbers taken from February HVCI.). Utilisation data will be redacted for sites with fewer than 5 customers. This will be second person reviewed.
2	Security	We use MDI, LV monitor and ADMD data as the baseline loading for secondary loading forecasts, which in turn have been used for ED2 secondary investment planning and LV flex tenders. We have confidence that all analysis has been done appropriately and that it well characterises the needs of the system. However, due to the size of the dataset, the quality of data in some cases and the tools/processes currently available, it is possible that sharing of the utilisation data exposes limitations on a transformer-by-transformer basis. This can also be used to challenge our business plan assumptions. GIS / location data is already shared. It was recognised previously that the data could be used maliciously to cause deliberate and coordinated network damage, however, aggregation of this with other data sources does not increase the likelihood of this. The sharing of customer information could highlight sites with maximum CI/CML impact.	Major	Possible	7	Restrict Use and Access	Significant	Unlikely	5	Caveat the data further. Namely to manage expectations about the accuracy of the secondary transformer utilisation data and explain the improvements that will be made with the rollout of LV monitoring data, with a signpost to progress on this. Sharing the data under a "shared data licence" would give us better ability to manage this messaging. This should reduce the stakeholder impact of this risk. There are ongoing network and cyber resilience reviews and investment to improve network security and strenghten resilience. In addition, although this risk exists, it is not considerably increased through release of this data set as parties with malicious intent could still access this information through LineSearch, Contestable UMV or in the case of above ground assets - visual inspection.
3	Public Interest	Stakeholders are likely to use this data (i.e. rating and utilisation in combination) to inform them of the best areas of the network to connect to. It will be possible to gain an indicative view, but lots of caveats apply. Assessing suitability of connection must also account for circuit constraints and local geography. It is possible that too much weight is placed on the conclusions drawn from this data, and stakeholders believe they are getting conflicting quotes/information from connections teams.	Moderate	Possible	5	Restrict Use and Access	Minor	Unlikely	3	Caveat the data. Namely, that rating is not a full measure of network constraints (e.g. circuit limitations), that local geographic constraints associated with new connections must still be considered, and that loading information does not necessarily account for connection agreements taken since the maximum demand was recorded. Sharing the data under a "shared data licence" would give us better ability to manage this messaging. This messaging should hopefully reduce the likelihood and extent to which data users use the data inappropriately. Note that the dataset will improve over ED2 - e.g. through improving circuit information records, development of the connections tool, as well as further development of the ENZ platform, which will represent an advanced network planning tool that relies on various network datasets.
4	Commercial	The data could be used to expose weaknesses or perceived weaknesses to media/press organisations. Furthermore, it is possible that data users could repackage data in the development of their own services/products/tools, which if not done correctly (or e.g. becomes out of date) could lead to greater stakeholder inconvenience. Information on primary peak demand at primary sites is already available (e.g. LTDS, DFES, Network Development Plan). External parties could look at the difference between this and the sum of the secondary sites, which may cause misinterpretation of data.	Moderate	Possible	5	Restrict Use and Access	Moderate	Unlikely	4	Data is being shared under a "shared data licence". This should prevent the repackaging of data. Enable process for managing these requests so we can have a clear register of who has been provisioned this information.
5	Legislation/Regulation Preventions	N/A	N/A	N/A	0	N/A	N/A	N/A	0	
6	Other	This contains commercial address information (the data is replicated by the data user internally, linked to the intended purpose, there is a risk that the data could become out of date, which may be the same as the individuals home address e.g. farm/sole trader). Disclosure of address could be used to identify high value plant & equipment that may be a security risk.	Moderate	Possible	5	Oher	Minor	Remote	2	Data on the platform would be kept up to date (see note 4). The users could be asked to confirm that they acknowledge the need to check back for updated data.

Overall Risk Score (without mitigation)	7.17

Overall Risk Score (with mitigation)	5.23

LIKELIHOOD RATINGS:

	Likelihood
	N/A
	Remote. Would only happen in exceptional circumstances e.g. there are no historical instances.
	Unlikely. There may have been potential cases/ near misses in the past.
	Possible. Known to have happened before on rare occassions, or has partially occurred.
	Expected. Has happened before and strong possibility it will likely occur again.
	Certain. Expected to occur frequently.

IMPACT RATINGS:

	Impact	**E.g. if in P&L and/or cash terms**	**Examples if in stakeholder terms. Reputation and relationships with employees; customers; shareholders, press, government, and/or regulators**
	N/a	N/a	N/a
	Minor. Would have insignificant impact.	< £1m	Short term loss of employee morale, local adverse publicity/media report.
	Moderate. Would have moderate impact which can be effectively managed.	£1m-£10m	Minor employee disengagement, prolonged local adverse publicity/media reporting, localised stakeholder concern, temporary drop in share price, minor reduction in customer base.
	Significant. May require intervention but further impact on any other critical assets/processes unlikely.	£10m-£25m	Isolated employee disengagement, business unit(s), national media interest creating stakeholder concern, negative national stakeholder statements, prolonged decrease in share price, moderate reduction in customer base.
	Major impact on key processes/ critical assets affected requiring immediate action to prevent long term damage to the organisation.	£25m-£50m	Employee disengagement across several business units, extensive prolonged adverse reactions from media and/or key stakeholders, significant decrease in share price, and a significant reduction in customer base.
	Catastrophic impact upon the business and/or wider industry and/or stakeholder. Reputational damage/ regulatory non-compliance.	>£50m	Company wide employee disengagement, downgrade in credit rating, extensive widespread negative reporting or public disputes with key stakeholders, loss of investor confidence, extensive reduction in customer base, escalation inevitable and impossible to contain.

RISK SCORING:

		IMPACT					
		Not Applicable	**Minor**	**Moderate**	**Significant**	**Major**	**Catastrophic**
LIKELIHOOD	**Not Applicable**	0	0	0	0	0	0
	Remote	0	2	3	4	5	6
	Unlikely	0	3	4	5	6	7
	Possible	0	4	5	6	7	8
	Expected	0	5	6	7	8	9
	Certain	0	6	7	8	9	10